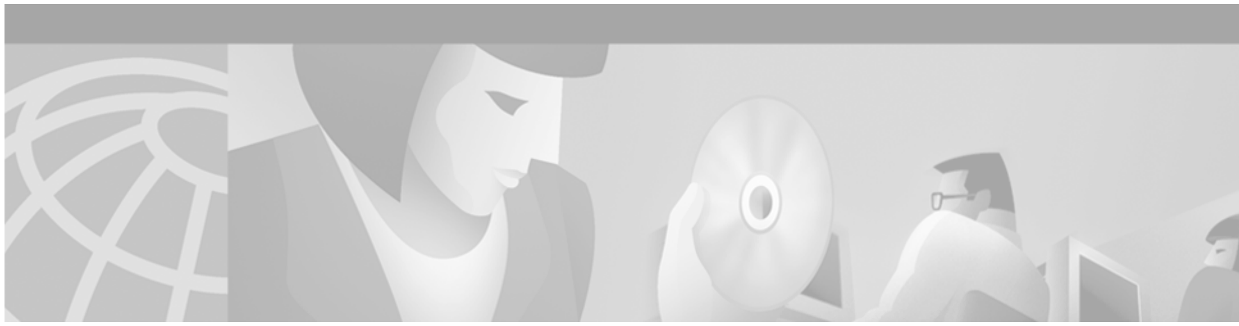

Cisco IOS Voice, Video, and Fax Commands: R Through Sh

This chapter presents the commands to configure and maintain Cisco IOS voice, video, and fax applications. The commands are presented in alphabetical order beginning with R. Some commands required for configuring voice, video, and fax may be found in other Cisco IOS command references. Use the command reference master index or search online to find these commands.

For detailed information on how to configure these applications and features, refer to the *Cisco IOS Voice, Video, and Fax Configuration Guide*.

register e164

To configure a gateway to register or deregister (remove the registration for) a fully qualified plain old telephone service (POTS) dial-peer E.164 address with a gatekeeper, use the **register e164** command in dial-peer configuration mode. To deregister an E.164 address, use the **no** form of this command.

register e164

no register e164

Syntax Description

This command has no keywords or arguments.

Defaults

No E.164 addresses are registered until you enter this command.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use this command to register the E.164 address of an analog telephone line attached to a Foreign Exchange Station (FXS) port on a router. The gateway automatically registers fully qualified E164 addresses. Use the **no register e164** command to deregister an address. Use the **register e164** command to register a deregistered address.

Before you automatically or manually register an E.164 address with a gatekeeper, you must create a dial peer (using the **dial-peer** command), assign an FXS port to the peer (using the **port** command), and assign an E.164 address (using the **destination-pattern** command). The E.164 address must be a fully qualified address. For example, +5551212, 5551212, and 4085551212 are fully qualified addresses; 408555.... is not a fully qualified address. E.164 addresses are registered only for active interfaces—those that are not shut down. If an FXS port or its interface is shut down, the corresponding E.164 address is deregistered.

Tips

You can use the **show gateway** command to find out if the gateway is connected to a gatekeeper and if a fully qualified E.164 address is assigned to the gateway. Use the **zone-prefix** command at the gatekeeper to define prefix patterns, such as 408555...., that apply to one or more gateways.

Examples

The following command sequence places the gateway in dial-peer configuration mode, assigns an E.164 address to the interface, and registers that address with the gatekeeper:

```
dial-peer voice 111 pots
 port 1/0/0
 destination-pattern 5551212
 register e164
```

The following commands deregister an address with the gatekeeper:

```
dial-peer voice 111 pots
no register e164
```

The following example shows that you must have a connection to a gatekeeper and define a unique E.164 address before you can register an address:

```
dial-peer voice 222 pots
port 1/0/0
destination 919555....
register e164


ERROR-register-e164:Dial-peer destination-pattern is not a full E.164 number

no gateway
dial-peer voice 111 pots
register e164


ERROR-register-e164:No gatekeeper
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dial-peer	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
port	Enables an interface on a PA-4R-DTR to operate as a concentrator port.
show gateway	Displays the current gateway status.
zone prefix	Configures the gatekeeper with knowledge of its own prefix and the prefix of any remote zone.

registered-caller ring

To configure the Nariwake service registered caller ring cadence, use the **registered-caller ring** command in dial-peer configuration mode.

registered-caller ring *cadence*

Syntax Description

cadence	A value of 0, 1, or 2. The default ring cadence for registered callers is 1 and for unregistered callers is 0. The on and off periods of ring 0 (normal ringing signals) and ring 1 (ringing signals for the Nariwake service) are defined in the NTT user manual.

Defaults

The default Nariwake service registered caller ring cadence is ring 1.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1.(2)XF	The command **registered-caller ring** was introduced on the Cisco 800 series routers.

Usage Guidelines

If your ISDN line is provisioned for the I Number or dial-in services, you must also configure a dial peer by using the **destination-pattern not-provided** command. Either port 1 or port 2 can be configured under this dial peer. The router then forwards the incoming call to voice port 1. (See the “Examples” section below.

If more than one dial peer is configured with the **destination-pattern not-provided** command, the router uses the first configured dial peer for the incoming calls. To display the Nariwake ring cadence setting, use the **show run** command.

Examples

The following example sets the ring cadence for registered callers to 2.

```
pots country jp
dial-peer voice 1 pots
 registered-caller ring 2
```

req-qos

To specify the desired quality of service to be used in reaching a specified dial peer, use the **req-qos** command in dial-peer configuration mode. To restore the default value for this command, use the **no** form of this command.

req-qos {**best-effort** | **controlled-load** | **guaranteed-delay**}

no req-qos

Syntax Description

best-effort	Indicates that Resource Reservation Protocol (RSVP) makes no bandwidth reservation.
controlled-load	Indicates that RSVP guarantees a single level of preferential service, presumed to correlate to a delay boundary. The controlled load service uses admission (or capacity) control to assure that preferential service is received even when the bandwidth is overloaded.
guaranteed-delay	Indicates that RSVP reserves bandwidth and guarantees a minimum bit rate and preferential queueing if the bandwidth reserved is not exceeded.

Defaults

best-effort

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series routers.

Usage Guidelines

This command is applicable only to VoIP dial peers.

Use the **req-qos** command to request a specific quality of service to be used in reaching a dial peer. Like **acc-qos**, when you issue this command, the Cisco IOS software reserves a certain amount of bandwidth so that the selected quality of service can be provided. Cisco IOS software uses Resource Reservation Protocol (RSVP) to request quality of service guarantees from the network.

Examples

The following example configures **guaranteed-delay** as the desired (requested) quality of service to a dial peer:

```
dial-peer voice 10 voip
 req-qos guaranteed-delay
```

Related Commands

Command	Description
acc-qos	Defines the acceptable QoS for any inbound and outbound call on a VoIP dial peer.

reset

To reset a set of digital signal processors (DSPs), use the **reset** command in global configuration mode.

reset *number*

Syntax Description

number	Specifies the number of DSPs to be reset. The number of DSPs ranges from 0 to 30.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

12.0(5)XE	This command was introduced on the Cisco 7200 series routers.
12.0(7)T	This command was integrated into the Cisco IOS Release 12.0(7)T.

Examples

The following example displays the **reset** command configuration for DSP 1:

```
reset 1
01:24:54:%DSPRM-5-UPDOWN: DSP 1 in slot 1, changed state to up
```

resource threshold

To configure a gateway to report H.323 resource availability to the its gatekeeper, use the **resource threshold** command in gateway configuration mode. To disable gateway resource-level reporting, use the **no** form of this command.

resource threshold [**all**] [**high** *percentage-value*] [**low** *percentage-value*]

no resource threshold

Syntax Description

all	(Optional) Applies the high- and low- parameter settings to all monitored H.323 resources. This is the default condition.
high *percentage-value*	(Optional) A resource utilization level that triggers a Resource Availability Indicator (RAI) message indicating that H.323 resource use is high. Enter a number between 1 and 100 that represents the high-resource utilization percentage. A value of 100 specifies high-resource usage when any H.323 resource is unavailable. The default is 90 percent.
low *percentage-value*	(Optional) Resource utilization level that triggers an RAI message indicating that H.323 resource usage has dropped below the high-usage level. Enter a number between 1 and 100 that represents the acceptable resource utilization percentage. After the gateway sends a high-utilization message, it waits to send the resource recovery message until the resource use drops below the value defined by the **low** parameter. The default is 90 percent.

Defaults

Reports low resources when 90 percent of resources are in use, and reports resource availability when resource use drops below 90 percent.

Command Modes

Gateway configuration

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

The **resource threshold** command defines the resource load levels that trigger Resource Availability Indicator (RAI) messages. To view the monitored resources, enter the **show gateway** command.

The monitored H.323 resources include digital signal processor (DSP) channels and DS0s. Use the **show call resource voice stats** command to see the total amount of resources available for H.323 calls.

Note The DS0 resources that are monitored for H.323 calls are limited to the ones that are associated with a voice POTS dial peer.

See the **dial-peer** configuration commands for details on how to associate a dial peer with a PRI or CAS group.

When any monitored H.323 resources exceed the threshold level defined by the **high** parameter, the gateway sends an RAI message to the gatekeeper with the AlmostOutOfResources field flagged. This message reports high resource usage.

When all gateway H.323 resources drop below the level defined by the **low** parameter, the gateway sends the RAI message to the gatekeeper with the AlmostOutOfResources field cleared.

When a gatekeeper can choose between multiple gateways for call completion, the gatekeeper uses internal priority settings and gateway resource statistics to determine which gateway to use. When all other factors are equal, a gateway that has available resources will be chosen over a gateway that has reported limited resources.

Examples

The following command defines the H.323 resource limits for a gateway:

```
resource threshold high 70 low 60
```

Related Commands

Command	Description
show call resource voice stats	Displays resource statistics for an H.323 gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.
show gateway	Displays the current gateway status.

response-timeout

To configure the maximum time to wait for a response from a server, use the **response-timeout** command in settlement configuration mode. To restore the default value of this command, use the **no** form of this command.

response-timeout *number*

no response-timeout *number*

Syntax Description

number	Response waiting time in seconds.

Defaults

The default response timeout is one (1) second.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no response is received within the response-timeout time limit, the current connection ends, and the router attempts to contact the next service point.

Examples

The following example illustrates a response-timeout set to 1 second.

```
settlement 0
 response-timeout 1
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.
url	Specifies the Internet service provider address.

retry-delay

To set the time between attempts to connect with the settlement provider, use the **retry-delay** command in settlement configuration mode. To restore the default value, use the **no** form of this command.

retry-delay *number*

no retry-delay

Syntax Description

number	Length of time (in seconds) between attempts to connect with the settlement provider. The valid range for retry delay is from 1 to 600 seconds.

Defaults

The default retry delay is two seconds.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 and 3600 series routers and the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

After exhausting all service points for the provider, the router is delayed for the specified length of time before resuming connection attempts.

Examples

The following example sets a retry value of 15 seconds:

```
settlement 0
 relay-delay 15
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after completion of a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-limit	Sets the maximum number of attempts to connect to the provider.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown/no shutdown	Deactivates the settlement provider/activates the settlement provider.
type	Configures an SAA-RTR operation type.

retry-limit

To set the maximum number of attempts to connect to the provider, use the **retry-limit** command in settlement configuration mode. To restore the default value, use the **no** form of this command.

retry-limit *number*

no retry-limit *number*

Syntax Description

number	Maximum number of connection attempts in addition to the first attempt.

Defaults

The default retry limit is one (1) retry.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no connection is established after the configured retries, the router ceases connection attempts. The retry limit number does not count the initial connection attempt. A retry limit of one (default) results in a total of two connection attempts to every service point.

Examples

The following example sets the number of retries to 1:

```
settlement 0
 retry-limit 1
```

Related Commands

Command	Description
connection-timeout	Configures the time for which a connection is maintained after a communication exchange is complete.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.

Command	Description
session-timeout	Sets the length of interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement mode and specifies the attributes specific to a settlement provider.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

retry (SIP user-agent)

To configure the number of retry attempts for Session Initiation Protocol (SIP) messages, use the **retry** command in SIP user-agent configuration mode. To reset this command to the default value, use the **no** form of this command.

retry {**invite** *number* | **response** *number* | **bye** *number* | **cancel** *number*}

no retry {**invite** *number* | **response** *number* | **bye** *number* | **cancel** *number*}

Syntax Description

invite *number*	Number of INVITE retries: 1 through 10 are valid inputs; default = 6.
response *number*	Number of RESPONSE retries: 1 through 10 are valid inputs; default = 6.
bye *number*	Number of BYE retries: 1 through 10 are valid inputs; default = 10.
cancel *number*	Number of CANCEL retries: 1 through 10 are valid inputs; default = 10.

Defaults

invite: 6
response: 6
bye: 10
cancel: 10

Command Modes

SIP user-agent configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

To reset this command to the default value, you can also use the **default** command.

Examples

In the following example, the number of invite retries has been set to 5.

```
sip-ua
 retry invite 5
```

Related Commands

Command	Description
sip-ua	Enables the sip-ua configuration commands, with which you configure the user agent.

ring

To set up a distinctive ring for your connected telephones, fax machines, or modems, use the **ring** command in interface configuration mode. To disable the specified distinctive ring, use the **no** form of this command.

ring *cadence-number*

no ring *cadence-number*

Syntax Description

cadence-number	Number from 0 through 2: • Type 0 is a primary ringing cadence—default ringing cadence for the country your router is in. • Type 1 is a distinctive ring—0.8 seconds on, 0.4 seconds off, 0.8 seconds on, 0.4 seconds off. • Type 2 is a distinctive ring—0.4 seconds on, 0.2 seconds off, 0.4 seconds on, 0.2 seconds off, 0.8 seconds on, 4 seconds off.

Defaults

The default is 0.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series router.

Usage Guidelines

This command applies to Cisco 800 series routers.

You can specify this command when creating a dial peer. This command will not work if it is not specified within the context of a dial peer. For information on creating a dial peer, refer to the *Cisco 800 Series Routers Software Configuration Guide*.

Examples

The following example specifies the type 1 distinctive ring:

```
ring 1
```

Related Commands

Command	Description
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the tag number associated with a dial peer.
no call-waiting	Disables call waiting.
port (dial-peer)	Enables an interface on a PA-4R-DTR port adapter to operate as a concentrator port.
pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (for Cisco 800 series routers).
ring	Sets up a distinctive ring for telephones, fax machines, or modems connected to a Cisco 800 series router.
show dial-peer voice	Displays configuration information and call statistics for dial peers.

ring cadence

To specify the ring cadence for a Foreign Exchange Station (FXS) voice port, use the **ring cadence** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

ring cadence {*pattern-number* | **define** *pulse interval*}

no ring cadence

Syntax Description

pattern-number	Predefined ring cadence patterns. Each pattern specifies a ring-pulse time and a ring-interval time. • **pattern01**—2 seconds on, 4 seconds off • **pattern02**—1 second on, 4 seconds off • **pattern03**—1.5 seconds on, 3.5 seconds off • **pattern04—**1 second on, 2 seconds off • **pattern05**—1 second on, 5 seconds off • **pattern06**—1 second on, 3 seconds off • **pattern07—**0.8 second on, 3.2 seconds off • **pattern08**—1.5 seconds on, 3 seconds off • **pattern09—**1.2 seconds on, 3.7 seconds off • **pattern09**—1.2 seconds on, 4.7 seconds off • **pattern11—**0.4 second on, 0.2 second off, 0.4 second on, 2 seconds off • **pattern12**—0.4 second on, 0.2 second off, 0.4 second on, 2.6 seconds off
define	User-definable ring cadence pattern. Each number pair specifies one ring-pulse time and one ring-interval time. You must enter numbers in pairs, and you can enter from 1 to 6 pairs. The second number in the last pair that you enter specifies the interval between rings.
pulse	A number (1 or 2 digits) specifying ring pulse (on) time in hundreds of milliseconds. The range is from 1 to 50, for pulses of 100 ms to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.
interval	A number (1 or 2 digits) specifying ring interval (off) time in hundreds of milliseconds. The range is from 1 to 50, for pulses of 100 to 5000 ms. For example: 1 = 100 ms; 10 = 1 s, 40 = 4 s.

Defaults

Ring cadence defaults to the pattern you specify with the **cptone** command.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers, and the **patternXX** keyword was introduced.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

The **patternXX** keyword provides preset ring cadence patterns for use on any platform. The **define** keyword allows you to create a custom ring cadence. On the Cisco 2600 and 3600 series routers, only one or two pairs of digits can be entered under the **define** keyword.

Examples

The following example configures the ring cadence for 1 second on and 4 seconds off on voice port 1/1 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/1
 ring cadence pattern02
```

The following example configures the ring cadence for 1 second on, 1 second off, 1 second on, and 5 seconds off on voice port 1/2 on a Cisco MC3810 multiservice concentrator:

```
voice-port 1/2
 ring cadence define 10 10 10 50
```

The following example configures the ring cadence for 1 second on and 2 seconds off on voice port 1/0/0 on a Cisco 2600 or 3600 series router:

```
voice-port 1/0/0
 ring cadence pattern04
```

Related Commands

Command	Description
ring frequency	Specifies the ring frequency for a specified FXS voice port.
cptone	Specifies the default tone, ring, and cadence settings according to country.

ring frequency

To specify the ring frequency for a specified Foreign Exchange Station (FXS) voice port, use the **ring frequency** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

ring frequency *number*

no ring frequency *number*

Syntax Description

number	Ring frequency (hertz) used in the FXS interface. Valid entries on the Cisco 3600 series are 25 and 50. Valid entries on the Cisco MC3810 multiservice concentrator are 20 and 30.

Defaults

25 Hz on the Cisco 3600 series routers and 20 Hz on the Cisco MC3810 multiservice concentrators.

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use the **ring frequency** command to select a specific ring frequency for an FXS voice port. Use the **no** form of this command to reset the default value. The ring frequency you select must match the connected equipment. If set incorrectly, the attached phone might not ring or might buzz. In addition, the ring frequency is usually country-dependent. You should take into account the appropriate ring frequency for your area before configuring this command.

This command does not affect ringback, which is the ringing a user hears when placing a remote call.

Examples

The following example configures the ring frequency on the Cisco 3600 series for 25 Hz:

```
voice-port 1/0/0
 ring frequency 25
```

The following example configures the ring frequency on the Cisco MC3810 multiservice concentrator for 20 Hz:

```
voice-port 1/1
 ring frequency 20
```

Related Commands

Command	Description
ring cadence	Specifies the ring cadence for an FXS voice port on the Cisco MC3810 multiservice concentrator.
ring number	Specifies the number of rings for a specified FXO voice port.

ring number

To specify the number of rings for a specified Foreign Exchange Office (FXO) voice port, use the **ring number** command in voice-port configuration mode. To restore the default value, use the **no** form of this command.

ring number *number*

no ring number *number*

Syntax Description

number	Number of rings detected before answering the call. Valid entries are numbers from 1 to 10. The default is 1.

Defaults

One ring

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.

Usage Guidelines

Use the **ring number** command to set the maximum number of rings to be detected before answering a call over an FXO voice port. Use the **no** form of this command to reset the default value, which is one ring.

Normally, this command should be set to the default so that incoming calls are answered quickly. If you have other equipment available on the line to answer incoming calls, you might want to set the value higher to give the equipment sufficient time to respond. In that case, the FXO interface would answer if the equipment online did not answer the incoming call in the configured number of rings.

This command is not applicable to Foreign Exchange Station (FXS) or E&M interfaces because they do not receive ringing on incoming calls.

Examples

The following example on the Cisco 3600 series sets five rings as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/0/0
 ring number 5
```

The following example on the Cisco MC3810 multiservice concentrator sets five rings as the maximum number of rings to be detected before closing a connection over this voice port:

```
voice-port 1/1
 ring number 5
```

Related Commands

Command	Description
ring frequency	Specifies the ring frequency for a specified FXS voice port.

roaming (dial-peer)

To enable the roaming capability for the dial peer, use the **roaming** command in dial-peer configuration mode. To disable the roaming capability, use the **no** form of this command.

roaming

no roaming

Syntax Description

This command has no arguments or keywords.

Defaults

No roaming

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server‘.

Usage Guidelines

Enable the roaming capability of a dial peer if that dial peer can terminate roaming calls. If a dial peer is dedicated to local calls only, disable the roaming capability.

The roaming dial peer must work with a roaming service provider. If the dial peer allows a roaming user to go through, and the service provider is not roaming-enabled, the call fails.

Examples

The following example enables the **roaming** capability for the dial peer:

```
dial-peer voice 10 voip
roaming
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified *provider-number.*
settlement roam-pattern	Configures a pattern to match against when determining roaming.

roaming (settlement)

To enable the roaming capability for a settlement provider, use the **roaming** command in settlement configuration mode. To disable the roaming capability, use the **no** form of this command.

roaming

no roaming

Syntax Description

This command has no arguments or keywords.

Defaults

No roaming

Command Modes

Settlement configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Enable roaming capability of a settlement provider if that provider can authenticate a roaming user and route roaming calls.

A roaming call is successful only if both the settlement provider and the outbound dial peer for that call are roaming-enabled.

Examples

The following example enables the roaming capability for the settlement provider:

```
settlement 0
roaming
```

Related Commands

Command	Description
roaming (dial-peer mode)	Enables the roaming capability for the dial peer.
settle-call	Limits the dial peer to using only the specific clearinghouse identified by the specified *provider-number*.
settlement roam-pattern	Configures a pattern to match against when determining roaming.

rtsp client session history duration

To specify how long to keep Real Time Streaming Protocol (RTSP) session history records in memory, use the **rtsp client session history duration** command in global configuration mode. To set the value to the default, use the **no** form of this command.

rtsp client session history duration *number*

no rtsp client session history duration *number*

Syntax Description

number	Specifies how long, in minutes, to keep the record.

Defaults

10 minutes

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Examples

The following example sets the RTSP session history to 500 minutes:

```
rtsp client session history duration 500
```

Related Commands

Command	Description
call application voice load	Allows reload of an aplication that was loaded via the MGCP scripting package.
rtsp client session history records	Specifies the number of RTSP client session history records kept during the session.
show call application voice	Displays all TCL or MGCP scripts that are loaded.
show rtsp client session	Displays cumulative information about the RTSP session records.

rtsp client session history records

To configure the number of records to keep in the RTSP client session history, use the **rtsp client session history records** command in global configuration mode. To set the value to the default, use the **no** form of this command.

rtsp client session history records *number*

no rtsp client session history records *number*

Syntax Description

number	Specifies the number of records to retain in a session history. Values range from 1 to 100000.

Defaults

50 records

Command Modes

Global configuration

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Examples

The following example sets the RTSP client history to 500 records:

```
rtsp client session history records 500
```

Related Commands

Command	Description
call application voice load	Allows reload of an aplication that was loaded via the MGCP scripting package.
rtsp client session history duration	Specifies the how long the RTSP is kept during the session.
show call application voice	Displays all TCL or MGCP scripts that are loaded.

rule

To apply a translation rule to a calling party number or a called party number for both incoming and outgoing calls, use the **rule** command in translation-rule configuration mode. To remove the translation rule, use the **no** form of this command.

rule *name-tag input-matched-pattern substituted-pattern* [*match-type substituted-type*]

no rule *name-tag input-matched-pattern substituted-pattern* [*match-type substituted-type*]

Syntax Description

name-tag	The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. Range is from 1 through 2147483647.
input-matched-pattern	The input string of digits for which pattern matching is performed.
substituted-pattern	The replacement digit string that results after pattern matching is performed. Regular expressions are used to carry out this process.
match-type	(Optional) The choices for this field are **international**, **national**, **subscriber**, **abbreviated**, **unknown**, and **any**, as defined by the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) Q.931 specification. If you enter the *match-type* value, then you must also enter the *substituted-type* value.
substituted-type	(Optional) The choices for this field are **international**, **national**, **subscriber**, **abbreviated** and **unknown**, as defined by the ITU Q.931 specification.

Note In the syntax description above, the square brackets indicate optional values. When using this command, do not include these square brackets as part of the syntax. They are not valid parameters in the **rule** command. The square brackets can only be used in actual syntax for such commands as the **destination-pattern** and **incoming called-number** commands, where the syntax specifically allows this delimiter.

Defaults

No default behavior or values.

Command Modes

Translation-rule configuration

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300 universal access server.
12.0(7)XKs	This command was first supported for Voice over IP on the following platforms: Cisco 2600 and 3600 series routers and Cisco MC3810 multiservice concentrators.

Release	Modification
12.1(1)T	This command was first supported on the T train for Voice over IP on the following platforms: Cisco 1750 routers, Cisco 2600 and 3600 series routers, Cisco AS5300 universal access servers, Cisco 7200 series routers, and Cisco 7500 series routers.
12.1(2)T	This command was first supported for Voice over IP on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

When configuring your dial peers, you are provided with an option called the *translation rule*. This option applies a translation rule to a calling party number (Automatic Number Identification [ANI]) or a called party number (Dial Number Information Service [DNIS]) for both incoming and outgoing calls within Cisco H.323 voice-enabled gateways. Also, the rule allows translation of the *type of number.*

Examples

The following example applies a translation rule. If a called number starts with 5552205 or 52205, then translation rule 21 will use the rule command to forward the number to 14085552205 instead.

```
translation-rule 21
 rule 1 555.% 1408555 subscriber international
 rule 2 7.% 1408555 abbreviated international
```

In the next example, if a called number is either 14085552205 or 014085552205, then after the execution of the translation rule 345, the forwarding digits will be 52205. If the match type is configured and the type is not “unknown,” then the dial peer matching will be required to match input string numbering type.

```
translation-rule 345
 rule 1 .%555.% 7 any abbreviated
```

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
test translation-rule	Tests the execution of the translation rules on a specific name tag.
translate	Applies a translation rule to a calling party number or a called party number for incoming calls
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

security

To enable authentication and authorization on a gatekeeper, use the **security** command in gatekeeper configuration mode. To disable security, use the **no** form of this command.

security {**any** | **h323-id** | **e164**} {**password default** *password* | **password separator** *character*}

no security {**any** | **h323-id** | **e164**} {**password default** *password* | **password separator** *character*}

Syntax Description

any	Uses the first alias of an incoming registration, admission, and status (RAS) protocol registration, regardless of its type, as the means of identifying the user to RADIUS/TACACS+.
h323-id	Uses the first H.323 ID type alias as the means of identifying the user to RADIUS/TACACS+.
e164	Uses the first E.164 address type alias as the means of identifying the user to RADIUS/TACACS+.
password default *password*	Specifies the default password that the gatekeeper associates with endpoints when authenticating them with an authentication server. The *password* must be identical to the password on the authentication server.
password separator *character*	Specifies the character that endpoints use to separate the H.323-ID from the piggybacked password in the registration. Specifying this character allows each endpoint to supply a user-specific password. The separator character and password will be stripped from the string before it is treated as an H.323-ID alias to be registered. Note that passwords may only be piggybacked in the H.323-ID, not the E.164 address, because the E.164 address allows a limited set of mostly numeric characters. If the endpoint does not wish to register an H.323-ID, it can still supply an H.323-ID consisting of just the separator character and password. This H.323-ID consisting of just the separator character and password will be understood to be a password mechanism and no H.323-ID will be registered.

Defaults

No default

Command Modes

Gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.

Usage Guidelines

Use the **security** command to enable identification of registered aliases by RADIUS/TACACS+. If the alias does not exist in RADIUS/TACACS+, the endpoint will not be allowed to register.

A RADIUS/TACACS+ server and encryption key must have been configured in Cisco IOS software for security to work.

Only the first alias of the proper type will be identified. If no alias of the proper type is found, the registration will be rejected.

This command does not allow you to define the password mechanism unless the security type (**h323-id** or **e164** or **any**) has been defined. Although the **no security password** command undefines the password mechanism, it leaves the security type unchanged, so security is still enabled. However, the **no security** command disables security entirely, including removing any existing password definitions.

Examples

The following example enables identification of registrations using the first H.323 ID found in any registration:

```
security h323id
```

The following example enables security, authenticating all users by using their H.323-IDs and a password of qwerty2x:

```
security h323-id
security password qwerty2x
```

The next example enables security, authenticating all users by using their H.323-IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security h323-id
security password separator !
```

Now if a user registers with an H.323-ID of joe!024aqx, the gatekeeper authenticates user joe with password 024aqx, and if that is successful, registers the user with the H.323-ID of joe. If the exclamation point is not found, the user is authenticated with the default password, or a null password if no default has been configured.

The following example enables security, authenticating all users by using their E.164 IDs and the password entered by the user in the H.323-ID alias he or she registers:

```
security e164
security password separator !
```

Now if a user registers with an E.164 address of 5551212 and an H.323-ID of !hs8473q6, the gatekeeper authenticates user 5551212 and password hs8473q6. Because the H.323-ID string supplied by the user begins with the separator character, no H.323-ID is registered, and the user is known only by the E.164 address.

Related Commands

Command	Description
accounting (gatekeeper)	Enables the accounting security feature on the gatekeeper.
radius-server host	Specifies a RADIUS server host.
radius-server key	Sets the authentication and encryption key for all RADIUS communications between the router and the RADIUS daemon.

sequence-numbers

To enable the generation of sequence numbers in each frame generated by the digital signal processor (DSP) for Voice over Frame Relay applications, use the **sequence-numbers** command in dial-peer configuration mode. To disable the generation of sequence numbers, use the **no** form of this command.

sequence-numbers

no sequence-numbers

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco 2600 and 3600 series routers and the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated into the Cisco IOS Release 12.0(4)T.

Usage Guidelines

Sequence numbers on voice packets allow the digital signal processor (DSP) at the playout side to detect lost packets, duplicate packets, or out-of-sequence packets. This helps the DSP to mask out occasional drop-outs in voice transmission at the cost of one extra byte per packet. The benefit of using sequence numbers versus the cost in bandwidth of adding an extra byte to each voice packet on the Frame Relay network must be weighed to determine whether to disable this function for your application.

Another factor to consider is that this command does not affect codecs that require a sequence number, such as G.726. If you are using a codec that requires a sequence number, the DSP will generate one regardless of the configuration of this command.

Examples

The following example shows how to disable the generation of sequence numbers for VoFR frames on a Cisco 2600 series or 3600 series router or on a Cisco MC3810 multiservice concentrator for VoFR dial peer 200, starting from global configuration mode:

```
dial-peer voice 200 vofr
 no sequence-numbers
```

Related Commands

Command	Description
called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
session protocol (Voice over Frame Relay)	Establishes a session protocol for calls between the local and remote routers via the packet network.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

server (RLM)

To identify an RLM server, use the **server** RLM configuration command. To remove the identification, use the **no** form of this command

server *name-tag*

no server *name-tag*

Syntax Description

name-tag	Name to identify the server configuration so that multiple entries of server configuration can be entered.

Defaults

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Usage Guidelines

Each server can have multiple entries of IP addresses or aliases.

Examples

The following example identifies the RLM server and defines the associated IP addresses:

```
rlm group 1
 server r1-server
 link address 10.1.4.1 source Loopback1 weight 4
 link address 10.1.4.2 source Loopback2 weight 3
```

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

server registration-port

To configure the listener port for the server to establish a connection with the gatekeeper, use the **server registration-port** command in gatekeeper configuration mode. To force the gatekeeper to close the listening socket so that no more new registration takes place, use the **no** form of this command.

server registration-port *port number*

no server registration-port *port number*

Syntax Description

port number	Specifies a single range of values from 1 through 65535 for the port number on which the gatekeeper listens for external server connections.

Defaults

The registration port of the gatekeeper is not configured, so no external server can register with this gatekeeper.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use this command to configure a server registration port to poll for servers that want to establish connections with the gatekeeper on this router.

Note The **no** form of this command forces the gatekeeper on this router to close the listen socket, so it cannot accept more registrations. However, existing connections between the gatekeeper and servers are left open.

Examples

The following example shows how a listener port for a server is established for connection with a gatekeeper:

```
server registration-port 20000
```

Related Commands

Command	Description
server trigger	Configure static server triggers for specific RAS messages to be forwarded to a specified server.

server trigger

To configure a static server trigger for external applications, use the **server trigger** command in gatekeeper configuration mode. To remove a single statically configured trigger entry, use the **no** form of this command. To remove every static trigger you configured if you want to delete them all, use the **all** keyword.

server trigger {**arq** | **lcf** | **lrj** | **lrq** | **rrq** | **urq**} *gkid priority server-id server-ipaddress server-port*

no server trigger {**arq** | **lcf** | **lrj** | **lrq** | **rrq** | **urq**} *gkid priority*

no server trigger all

Syntax Description

all	Specified to delete all command-line interface configured triggers.
arq, lcf, lrj, lrq, rrq, urq	Registration, admission, and status (RAS) protocol message types. Use these message types to specify a submode in the gatekeeper configuration mode in which you configure a trigger for the gatekeeper to act upon. Specify only one message type per server trigger command. There is a different trigger submode for each message type. Each trigger submode has its own set of applicable commands.
gkid	The local gatekeeper identifier.
priority	The priority for each trigger. The range is from 1 through 20, with 1 being the highest priority.
server-id	The ID number of the external application.
server-ipaddress	The IP address of the server.
server-port	The port on which the Cisco IOS gatekeeper listens for messages from the external server connection.

Defaults

No server triggers are set.

Command Modes

Gatekeeper configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Use this command to configure a static server trigger. There are six different server triggers—one for each of the RAS messages. To configure a trigger, go to its submode where a set of subcommands are used to trigger a condition. See the following examples.

In ARQ submode, enter the following syntax:

```
server trigger arq gkid priority server-id server-ipaddress server-port
```

In LCF submode, enter the following syntax:

```
server trigger lcf gkid priority server-id server-ipaddress server-port
```

In LRJ submode, enter the following syntax:

```
server trigger lrj gkid priority server-id server-ipaddress server-port
```

In LRQ submode, enter the following syntax:

```
server trigger lrq gkid priority server-id server-ipaddress server-port
```

In RRQ submode, enter the following syntax:

```
server trigger rrq gkid priority server-id server-ipaddress server-port
```

In URQ submode, enter the following syntax:

```
server trigger urq gkid priority server-id server-ipaddress server-port
```

The following options are available in all submodes:

info-only	Information only—no need to wait for acknowledgment.
shutdown	Enter this subcommand to temporarily disable a trigger. The gatekeeper does not consult triggers in a shutdown state when determining what message to forward.

The *destination-info* argument is under the ARQ, LRQ, LCF, and LRJ submode and has the following options:

destination-info	Configure *destination-info* to trigger one of the following conditions:
e164	Configure an E.164 pattern.
email-id	Configure an email ID.
h323-id	Configure an H.323 ID.
word	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing ‘., ‘s, or ‘*’.

The *redirect-reason* argument is under the ARQ and LRQ submodes and has the following options:

redirect-reason	Configure a *redirect-reason* to trigger on (range of 0 through 65535) with the following reserved values:
0	Unknown reason.
1	Call forwarding busy or called DTE busy.
2	Call forwarded no reply.
4	Call deflection.
9	Called DTE out of order.
10	Call forwarding by the call DTE.
15	Call forwarding unconditionally.

The *remote-ext-address* argument is under the LCF trigger submode and has the following options:

remote-ext-address	Configure remote extension addresses, with the following options:
e164	Configure an E.164 pattern.
word	When configuring the e164 address option, the email-id option, or the h323-id option above, the E.164 address can end in a trailing '., 's, or '*'.

The *endpoint-type* argument is under the RRQ and URQ trigger submodes and has the following options:

endpoint-type	Configure the type of endpoint to trigger, with the following options:
gatekeeper	The endpoint is an H.323 gatekeeper.
h320-gateway	The endpoint is an H.320 gateway.
mcu	The endpoint is a multipoint control unit (MCU).
other-gateway	The endpoint is another type of gateway not specified on this list.
proxy	The endpoint is a H.323 proxy.
terminal	The endpoint is an H.323 proxy.
voice-gateway	The endpoint is a voice gateway.

The **supported-prefix** keyword is under the RRQ and URQ submodes and has the following options:

supported-prefix	Configure the gateway technology prefix to trigger on.
word	Enter a word within the set of "0123456789#*" when configuring the E.164 pattern for a gateway technology prefix.

Entering the **no** form of the server trigger command removes the trigger definition from the Cisco IOS gatekeeper with all statically configured conditions under that trigger.

Examples

The following example configures a server trigger on gatekeeper sj.xyz.com to notify external server "Server-123" of any call to an E.164 number that starts with 1800 followed by any 7 digits (1800551212, for example):

```
Gatekeeper
  server trigger arq sj.xyz.com 1 Server-123 1.14.93.130 1751
    destination-info e164 1800.......
    exit
```

Related Commands

Command	Description
server registration port	Configure a gatekeeper listening port to listen for external server connections.
show gatekeeper servers	Show a list of currently registered and statically configured triggers on this gatekeeper router.

session

To associate a transport session with a specified session-group, use the **session group** command in backhaul session manager configuration mode. It is assumed that the server is located on a remote machine. To delete the session, use the **no** form of this command.

session group *group-name remote_ip remote_port local_ip local_port priority*

no session group *group-name remote_ip remote_port local_ip local_port priority*

Syntax Description

group	Specifies the session-group name.
group-name	Session-group name.
remote_ip	Remote IP address.
remote_port	Remote port number. Range is 1024 through 9999.
local_ip	Local IP address.
local_port	Local port number. Range is 1024 through 9999.
priority	Priority of the session-group. Range is 0 through 9999 and 0 is the highest priority.

Defaults

No default behavior or values.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.
12.2(2)XB1	This command was implemented on the Cisco AS5850 platform.

Examples

To associate a transport session with the session-group Group5 and specify the parameters described above, see the following example:

```
Router(config-bsm)# session group group5 161.44.2.72 5555 172.18.72.198 5555 1
```

session protocol

To specify a session protocol for calls between the local and remote routers using the packet network, use the **session protocol** command in dial-peer configuration mode. To reset the default value for this command, use the **no** form of this command.

session protocol {**cisco** | **sipv2** | **aal2-trunk** | **smtp**}

no session protocol

Syntax Description

cisco	Configure the dial peer to use proprietary Cisco VoIP session protocol.
sipv2	SIP users should use this option. This option configures the VoIP dial peer to use IETF SIP.
aal2-trunk	AAL2 nonswitched trunk session protocol.
smtp	Specifies Simple Mail Transfer Protocol (SMTP) session protocol.

Defaults

No default behaviors or values.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300 universal access server.
12.1(1)T	The **sipv2** option was added.
12.1(1)XA	Support was added for VoATM dial peers on the Cisco MC3810 multiservice concentrator with the **aal2-trunk** keyword.
12.1(2)T	Modifications to this command in Cisco IOS Release 12.1(1)XA were integrated into Cisco IOS Release 12.1(2)T.

Usage Guidelines

The keyword **cisco** is applicable only to VoIP on the Cisco 3600 series routers. The keyword **aal2-trunk** is applicable only to VoATM on the Cisco MC3810 multiservice concentrator.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is an example of configuring a VoIP dial peer for H.323 or SIP as the session protocol for VoIP call signaling:

```
dial-peer voice 102 voip
 session protocol sipv2
```

The following example selects AAL2 trunking as the session protocol on a Cisco MC3810 multiservice concentrator:

```
dial-peer voice 10 voatm
 session protocol aal2-trunk
```

The following example selects Cisco Session Protocol as the session protocol on a Cisco 3600 series router:

```
dial-peer voice 20 voip
 session protocol cisco
```

The following example selects SMTP as the session protocol:

```
dial-peer voice 10 mmoip
 session protocol smtp
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode and specifies the method of voice-related encapsulation.
session target (VoIP)	Configures a network-specific address for a dial peer.

session protocol (Voice over Frame Relay)

To establish a Voice over Frame Relay protocol for calls between the local and remote routers via the packet network, use the **session protocol** command in dial-peer configuration mode. To reset the default value, use the **no** form of this command.

session protocol {**cisco-switched** | **frf11-trunk**}

no session protocol

Syntax Description

cisco-switched	Specifies proprietary Cisco VoFR session protocol. (This is the only valid session protocol for the Cisco 7200 series.)
frf11-trunk	Specifies FRF.11 session protocol.

Defaults

cisco-switched

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced for VoIP.
12.0(3)XG	This command was modified to support VoFR on the Cisco 2600, 3600, and 7200 series routers and the Cisco MC3810 multiservice concentrator.
12.0(4)T	The **cisco-switched** and **frf11-trunk** keywords were added for VoFR dial peers.

Usage Guidelines

For Cisco-to-Cisco dial peer connections, Cisco recommends that you use the default session protocol because of the advantages it offers over a pure FRF.11 implementation. When connecting to FRF.11-compliant equipment from other vendors, use the FRF.11session protocol.

Note When using the FRF.11 session protocol on Cisco 2600 series and 3600 series routers, you must also use the **called-number** command.

Examples

The following example shows how to configure the FRF.11 session protocol on a Cisco 2600 series or 3600 series router for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 session protocol frf11-trunk
 called-number 5552150
```

The following example shows how to configure the FRF.11 session protocol on a Cisco MC3810 multiservice concentrator for VoFR dial peer 200:

```
dial-peer voice 200 vofr
 session protocol frf11-trunk
```

Related Commands

Command	Description
called-number (dial-peer)	Enables an incoming VoFR call leg to get bridged to the correct POTS call leg when using a static FRF.11 trunk connection.
codec (dial-peer)	Specifies the voice coder rate of speech for a Voice over Frame Relay dial peer.
cptone	Specifies a regional analog voice interface-related tone, ring, and cadence setting.
destination-pattern	Specifies either the prefix, the full E.164 telephone number, or an ISDN directory number (depending on the dial plan) to be used for a dial peer.
dtmf-relay (Voice over Frame Relay)	Enables the generation of FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred order of a dial peer within a rotary hunt group.
session target	Specifies a network-specific address for a specified dial peer or destination gatekeeper.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session protocol aal2

To enter the voice-service-session configuration mode and specify AAL2 trunking on a Cisco MC3810 multiservice concentrator, use the **session protocol aal2** command in voice-service configuration mode.

session protocol aal2

Syntax Description

This command has no keywords or arguments.

Defaults

There is no default setting for this command.

Command Modes

Voice-service configuration

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

This command applies to VoATM on the MC3810 multiservice concentrator.

In the voice-service-session configuration mode for AAL2, you can configure only AAL2 features, such as call admission control and subcell multiplexing.

Examples

The following example shows how to access the voice-service-session configuration mode, beginning in global configuration mode:

```
voice service voatm
  session protocol aal2
```

session protocol multicast

To set the session protocol as multicast, use the **session protocol multicast** command dial-peer configuration mode. To negate this command and return to the Cisco default session protocol, use the **no** version of this command.

session protocol multicast

no session protocol multicast

Syntax Description

There are no keywords or arguments.

Defaults

When this command is not implemented, the default session protocol is **cisco**.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(2)XH	This command was introduced on Cisco 2600 and Cisco 3600 series routers for the Cisco Hoot and Holler over IP application.
12.1(3)T	This command was integrated into the Cisco IOS Release 12.1(3)T.

Usage Guidelines

Use the **session protocol multicast** dial-peer configuration command for voice conferencing in a Hoot and Holler networking implementation. This command allows more than two ports to join the same session simultaneously. It is supported on Cisco 2600 and Cisco 3600 series routers.

Examples

The following example shows the use of the **session protocol multicast** dial-peer configuration command in context with its accompanying commands:

```
dial-peer voice 111 voip
 destination-pattern 111
 session protocol multicast
 session target ipv4:237.111.0.111:22222
 ip precedence 5
 codec g711ulaw
```

Related Commands

Command	Description
session target ipv4	Assigns the session target for voice-multicasting dial peers.

session target (VoATM)

To specify a network-specific address for a specified VoATM dial peer, use the **session target** command in dial-peer configuration mode. To restore default values for this parameter, use the **no** form of this command.

Cisco 3600 Series Routers Voice over ATM Dial Peers

session target *interface* **pvc** {*name* | *vpi/vci* | *vci*}

no session target

Cisco MC3810 Multiservice Concentrator Voice over ATM Dial Peers

session target {**serial** | **atm**} *interface* **pvc** {*word* | *vpi*/*vci* | *vci*} *cid*

no session target

Syntax Description

serial	Specifies the serial interface for the dial-peer address.
atm	Specifies the ATM interface. The only valid number is 0.
interface	Interface type and interface number on the router.
pvc	The specific ATM permanent virtual circuit (PVC) for this dial peer.
word	(Optional) A name that identifies the PVC. The argument can identify the PVC if a word identifier was assigned when the PVC was created.
name	The PVC name.
vpi/vci	ATM network virtual path identifier (VPI) and virtual channel identifier (VCI) of this PVC. On the Cisco 3600, if you have the Multiport T1/E1 ATM network module with IMA installed, the valid range for *vpi* is from 0 to 5, and the valid range for *vci* is from 1 to 255. If you have the OC3 ATM Network Module installed, the valid range for *vpi* is from 0 to 15, and the valid range for *vci* is from 1 to 1023.
vci	ATM network virtual channel identifier (VCI) of this PVC.
cid	ATM network channel identifier (CID) of this PVC. The valid range is from 8 to 255.

Defaults

The default for this command is enabled with no IP address or domain name defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	Support was added for VoATM, VoHDLC, and POTS dial peers on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	Support was added for VoATM dial peers on the Cisco 3600 series routers. Support for VoHDLC on the Cisco MC3810 multiservice concentrator was removed.
12.1(2)T	Support was added for VoATM on Cisco MC3810 multiservice concentrators.

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point will depend on the call origin and the loopback type selected.

This command applies to on-ramp store-and-forward fax functions.

You must enter the **session protocol aal2-trunk** dial-peer configuration command before you can specify a *cid* for a dial peer for VoATM on the Cisco MC3810 multiservice concentrator.

Note This command does not apply to plain old telephone service (POTS) dial peers.

Examples

The following example configures a session target for Voice over ATM on a Cisco MC3810 multiservice concentrator. The session target is sent to ATM interface 0, and for a PVC with a VCI of 20.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm0 pvc 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

The following example displays configuring a session target for Voice over ATM on the Cisco 3600 series. The session target is sent to ATM interface 0, and is for a PVC with a VPI/VCI of 1/100.

```
dial-peer voice 12 voatm
 destination-pattern 13102221111
 session target atm1/0 pvc 1/100
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoFR)

To specify a network-specific address for a specified VoFR dial peer, use the **session target** command in dial-peer configuration mode. To restore default values for this parameter, use the **no** form of this command.

Cisco 2600 and 3600 Series Routers Voice over Frame Relay Dial Peers

session target *interface dlci* [*cid*]

no session target

Cisco MC3810 Multiservice Concentrator Voice over Frame Relay Dial Peers

session target *interface dlci* [*cid*]

no session target

Cisco 7200 Series Routers Voice over Frame Relay Dial Peers

session target *interface dlci*

no session target

Syntax Description

interface	Specifies the serial interface and interface number (slot number and port number) associated with this dial peer. For the range of valid interface numbers for the selected interface type, enter a **?** character after the interface type.
dlci	Specifies the data link connection identifier for this dial peer. The valid range is from 16 to 1007.
cid	(Optional) Specifies the DLCI subchannel to be used for data on FRF.11 calls. A CID must be specified only when the session protocol is **frf11-trunk**. When the session protocol is **cisco-switched**, the CID is dynamically allocated. The valid range is from 4 to 255. **Note** By default, CID 4 is used for data; CID 5 is used for call-control. We recommend that you select CID values between 6 and 63 for voice traffic. If the CID is greater than 63, the FRF.11 header will contain an extra byte of data.

Defaults

The default for this command is enabled with no IP address or domain name defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	Support was added for VoFR, VoHDLC, and POTS dial peers on the Cisco MC3810 multiservice concentrator.
12.0(3)XG	Support was added for VoFR dial peers on the Cisco 2600 series and 3600 series routers. The *cid* option was added.
12.0(4)T	Support was added for VoFR and POTS dial peers on the Cisco 7200 series routers and the support added in Cisco IOS Release 12.0(3)XG was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select. The syntax of this command complies with the simple syntax of mailto: as described in RFC 1738.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point will depend on the call origin and the loopback type selected.

For VoFR dial peers, the *cid* option is not allowed when the **cisco-switched** option for the **session protocol** command is used.

Examples

The following example configures a session target for Voice over Frame Relay on a Cisco MC3810 multiservice concentrator with a session target on serial port1 and a DLCI of 200:

```
dial-peer voice 11 vofr
 destination-pattern 13102221111
 session target serial1 200
```

The following example shows how to configure serial interface 1/0, DLCI 100 as the session target for VoFR dial peer 200 (an FRF.11 dial peer) on a Cisco 2600 series or 3600 series router, starting from global configuration mode and using the FRF.11 session protocol:

```
dial-peer voice 200 vofr
 destination-pattern 13102221111
 called-number 5552150
 session protocol frf11-trunk
 session target serial 1/0 100 20
```

The following example delivers fax-mail to multiple recipients:

```
dial-peer voice 10 mmoip
 session target marketing-information@mailer.example.com
```

Assuming that mailer.example.com is running sendmail, you can put the following information into its /etc/aliases file:

```
marketing-information:
 john@example.com,
 fax=+14085551212@sj-offramp.example.com
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
session protocol	Establishes a VoFR protocol for calls between the local and the remote routers via the packet network.
signal-type	Sets the signaling type to be used when connecting to a dial peer.

session target (VoIP)

To specify a network-specific address for a specified VoIP dial peer, use the **session target** command in dial-peer configuration mode. To restore default values for this parameter, use the **no** form of this command.

Cisco 2600 and Cisco 3600 Series Routers and Cisco MC8310 Multiservice Concentrator Voice over IP Dial Peers

session target {**ipv4:***destination-address* | **dns:**[**s.** | **d.** | **e.** | **u.**] *host-name* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed** | **ras** | **settlement**}

no session target

Cisco AS5300 Universal Access Server Voice over IP Dial Peers

session target {**ipv4:***destination-address* | **dns:**[**s.** | **d.** | **e.** | **u.**] *host-name* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed** | **mailto:** | {*name* | **d**}@*domain-name* | **ipv4:***destination-address* | **dns:**[**s.** | **d.** | **u.** | **e.**] *host-name*}

no session target

Cisco AS5800 Universal Access Server Voice over IP Dial Peers

session target {**ipv4:***destination-address* | **dns:**[**s.** | **d.** | **e.** | **u.**] *host-name* | **loopback:rtp** | **loopback:compressed** | **loopback:uncompressed**}

no session target

Syntax Description

ipv4:*destination-address*	IP address of the dial peer.
dns:[**s...**] *host-name*	Indicates that the domain name server will be used to resolve the name of the IP address. Valid entries for this parameter are characters representing the name of the host device. (Optional) Use one of the following three wildcards with this keyword when defining the session target for Voice over IP (VoIP) peers: **s.**—Indicates that the source destination pattern will be used as part of the domain name. **d.**—Indicates that the destination number will be used as part of the domain name. **e.**—Indicates that the digits in the called number will be reversed, periods will be added between the digits of the called number, and this string will be used as part of the domain name. **u.**—Indicates that the unmatched portion of the destination pattern (such as a defined extension number) will be used as part of the domain name.
loopback:rtp	Indicates that all voice data will be looped back to the source. This is applicable for VoIP peers.
loopback:compressed	Indicates that all voice data will be looped back in compressed mode to the source. This is applicable for POTS peers.

loopback:uncompressed	Indicates that all voice data will be looped-back in uncompressed mode to the source. This is applicable for POTS peers.
ras	Indicates that the registration, admission, and status (RAS) signaling function protocol is being used, meaning that a gatekeeper will be consulted to translate the E.164 address into an IP address.
settlement *provider-number*	Indicates that the settlement server is the target to resolve the terminating gateway address. Enter the provider IP address for provider number.

Defaults

The default state for this command is enabled, with no IP address or domain name defined.

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
12.0(3)T	Support was added for VoIP and POTS dial peers on the Cisco AS5300 universal access server. The parameter was added for RAS.
12.0(4)XJ	Support was added for store-and-forward fax on the Cisco AS5300 universal access server platform.
12.1(1)T	Support was added for **session target** *type* of **settlement.**

Usage Guidelines

Use the **session target** command to specify a network-specific address or domain name for a dial peer. Whether you select a network-specific address or a domain name depends on the session protocol you select.

The **session target loopback** command is used for testing the voice transmission path of a call. The loopback point will depend on the call origin and the loopback type selected.

The **session target dns** command can be used with or without the specified wildcards. Using the optional wildcards can reduce the number of VoIP dial peer session targets you must configure if you have groups of numbers associated with a particular router.

Use the **session target ras** command to specify that the RAS protocol is being used to determine the IP address of the session target.

In Cisco IOS Release 12.1(1)T the **session target** command configuration cannot combine the target of RAS with the **settle-call** command. When configuring the VoIP dial peers for a settlement server, if **session target** *type* is **settlement**, the *provider-number* parameter in the **session target** and **settle-call** commands should be identical.

When the VoIP dial peers are configured for a settlement server, if the **session target** *type* is **settlement**, the *provider-number* parameter in the **session target** and **settle-call** commands should be identical.

Examples

The following example configures a session target using DNS for a host, “voice_router,” in the domain cisco.com:

```
dial-peer voice 10 voip
```

```
 session target dns:voice_router.cisco.com
```

The following example configures a session target using DNS, with the optional **u.** wildcard. In this example, the destination pattern has been configured to allow for any four-digit extension, beginning with the numbers 1310222. The optional wildcard **u.** indicates that the router will use the unmatched portion of the dialed number—in this case, the four-digit extension—to identify the dial peer. As in the preceding example, the domain is "cisco.com."

```
dial-peer voice 10 voip
 destination-pattern 1310222....
 session target dns:$u$.cisco.com
```

The following example configures a session target using DNS, with the optional **d.** wildcard. In this example, the destination pattern has been configured for 13102221111. The optional wildcard **d.** indicates that the router will use the destination pattern to identify the dial peer in the "cisco.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 13102221111
 session target dns:$d$.cisco.com
```

The following example configures a session target using DNS, with the optional **e.** wildcard. In this example, the destination pattern has been configured for 12345. The optional wildcard **e.** indicates that the router will reverse the digits in the destination pattern, add periods between the digits, and then use this reverse-exploded destination pattern to identify the dial peer in the "cisco.com" domain.

```
dial-peer voice 10 voip
 destination-pattern 12345
 session target dns:$e$.cisco.com
```

The following example configures a session target using RAS:

```
dial-peer voice 11 voip
 destination-pattern 13102221111
 session target ras
```

The following example configures a session target using settlement:

```
session target settlement:0
```

Related Commands

Command	Description
called-number	Enables an incoming VoFR call leg to be bridged to the correct POTS call leg.
codec (dial-peer)	Specifies the voice coder rate of speech for a dial peer.
cptone	Specifies a regional tone, ring, and cadence setting for an analog voice port.
dtmf-relay	Enables the DSP to generate FRF.11 Annex A frames for a dial peer.
preference	Indicates the preferred selection order of a dial peer within a hunt group.
signal-type	Sets the signaling type to be used when connecting to a dial peer.
destination-pattern	Specifies either the prefix or the full E.164 telephone number (depending on your dial plan) to be used for a dial peer.
session protocol	Establishes a session protocol for calls between the local and remote routers through the packet network in Voice over IP.
settle-call	Specifies that settlement is to be used for this dial peer, regardless of session target type.

session transport

To configure the VoIP dial peer to use TCP or User Datagram Protocol (UDP) as the underlying transport layer protocol for Session Initiation Protocol (SIP) messages, use the **session transport** command in dial-peer configuration mode. To reset the value to the default, use the **no** form of this command.

session transport {**udp** | **tcp** }

Syntax Description

udp	Configure the SIP dial peer to use the UDP transport layer protocol. This is the default.
tcp	Configure the SIP dial peer to use the TCP transport layer protocol.

Defaults

The SIP dial peer uses UDP.

Note The transport protocol specified with the **transport** command and the one specified with the **session transport** command must be the same.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Use **show sip-ua status** to ensure that the transport protocol that you set using the **session transport** command matches the protocol set using the **transport** command.

Examples

The following example shows a VoIP dial peer configured to use UDP as the underlying transport layer protocol for SIP messages:

```
dial-peer voice 102 voip
 session transport udp
```

set

To create a fault-tolerant or non-fault-tolerant session-set with the client or server option, use the **set** command in backhaul session manager configuration mode. To delete the set, use the **no** form of this command.

set *set-name* **{ client | server } { ft | nft }**

no set *set-name* **{ client | server } { ft | nft }**

Syntax Description

set-name	Session-set name.
client	Client option. The session-set should only be configured as client for backhaul.
server	Server option.
ft	Fault-tolerant. Fault-tolerance is the level of ability within a system to operate properly even if a group in the set fails.
nft	Non-fault-tolerant. Only one group is allowed in a non-fault-tolerant set.

Defaults

No default behavior or values.

Command Modes

Backhaul session manager configuration

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

There can be multiple groups associated with a session-set.

The session-set should only be configured for the client for backhaul (not the server).

A set cannot be deleted unless the groups associated with the set are deleted first.

Examples

To specify the client set named Set1 to fault-tolerant, see the following example:

```
Router(config-bsm)# set set1 client ft
```

settle-call

To force a call to be authorized with a settlement server that uses the address resolution method specified in the **session target** *type* command, use the **settle-call** command in dial-peer configuration mode. To make sure that no authorization will be performed by a settlement server, use the **no** form of this command.

settle-call *provider-number*

no settle-call *provider-number*

Syntax Description

provider-number	Digit defining the ID of a particular settlement server. The only valid entry is 0. **Note** If **session target** *type* is **settlement**, the *provider-number* argument in the **session target** and **settle-call** commands should be identical.

Defaults

No default behavior or values.

Command Modes

Dial-peer configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Using the **session target** command, a dial peer can determine the address of the terminating gateway through the **ipv4**, **dns**, **ras,** and **settlement** keywords.

If the session target is not **settlement,** and the **settle-call** *provider-number* argument is set, the gateway resolves the terminating gateway's address using the specified method and then requests the settlement server to authorize that address and create a settlement token for that particular address. If the server cannot authorize the terminating gateway address suggested by the gateway, the call fails.

Do not combine the session target types **ras** and **settle-call**. Combination of session target types is not supported in Cisco IOS Release 12.1(1)T.

Examples

The following example sets a call to be authorized with a settlement server that uses the address resolution method specified in the **session target**:

```
dial-peer voice 10 voip
 destination-pattern 1408.......
 session target ipv4:172.22.95.14
 settle-call 0
```

Related Commands

Command	Description
session target	Specifies a network-specific address for a specified dial peer.

settlement

To enter settlement configuration mode and specify the attributes specific to a settlement provider, use the **settlement** command in global configuration mode. To disable the settlement provider, use the **no** form of this command.

settlement *provider-number*

no settlement *provider-number*

Syntax Description

provider-number	Specifies a digit that defines a particular settlement server. The only valid entry is 0.

Defaults

0

Command Modes

Global configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The variable *provider-number* defines a particular settlement provider. For Cisco IOS Release 12.1, only one clearinghouse per system is allowed, and the only valid value for *provider-number* is 0.

Examples

This example shows how to enter settlement configuration mode:

```
settlement 0
```

Related Commands

Command	Description
connection-timeout	Configures the length of time for which a connection is maintained after a communication exchange is completed.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
retry-limit	Sets the connection retry limit.

Command	Description
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
show settlement	Displays the configuration for all settlement server transactions.
shutdown	Brings up the settlement provider.
type	Configures an SAA-RTR operation type.

settlement roam-pattern

To configure a pattern that must be matched to determine if a user is roaming, use the **settlement roam-pattern** command in global configuration mode. To delete a particular pattern, use the **no** form of this command.

settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **no roaming**}

no settlement *provider-number* **roam-pattern** *pattern* {**roaming** | **no roaming**}

Syntax Description

provider-number	Digit defining the ID of particular settlement server. The only valid entry is 0.
pattern	Specifies a user account pattern.
roaming | no roaming	Determines whether a user is roaming.

Defaults

No default pattern

Command Modes

Global configuration

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.

Usage Guidelines

Multiple "roam patterns" could be entered on one gateway.

Examples

The following example will configure a pattern that determines if a user is roaming:

```
settlement 0 roam-pattern 1222 roam
settlement 0 roam-pattern 1333 noroam
settlement roam-pattern 1444 roam
settlement roam-pattern 1555 noroam
```

Related Commands

Command	Description
roaming (settlement)	Enables the roaming capability for a settlement provider.
settlement	Enters settlement configuration mode.

sgcp

To start and allocate resources for the Simple Gateway Control Protocol (SGCP) daemon, use the **sgcp** command in global configuration mode. To terminate all calls, release all allocated resources, and kill the SGCP daemon, use the **no** form of this command.

sgcp

no sgcp

Syntax Description

This command has no arguments or keywords.

Defaults

The SGCP daemon is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

When the SGCP daemon is not active, all SGCP messages are ignored.

When you enter the **no sgcp** command, the SGCP process is removed.

Note After you enter the **no sgcp** command, you must save the configuration and reboot the router for the disabling of SGCP to take effect.

Examples

The following example shows the SGCP daemon being enabled:

```
sgcp
```

The following example shows the SGCP daemon being disabled:

```
no sgcp
```

Related Commands

Command	Description
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp call-agent

To define the IP address of the default Simple Gateway Control Protocol (SGCP) call agent in the router configuration file, use the **sgcp call-agent** command in global configuration mode. To remove the IP address of the default SGCP call agent from the router configuration, use the **no** form of this command.

sgcp call-agent *ipaddress* [**:***udp port*]

no sgcp call-agent *ipaddress*

Syntax Description

ipaddress	Specifies the IP address or hostname of the call agent.
:*udp port*	(Optional) Specifies the UDP port of the call agent.

Defaults

No IP address is configured.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Setting this command defines the IP address of the default SGCP call agent to which the router sends an initial RSIP (Restart In Progress) packet when the router boots up. This is used for initial boot-up only before the SGCP call agent contacts the router acting as the gateway.

When you enter the **no sgcp call-agent** command, only the IP address of the default SGCP call agent is removed.

Examples

The following example shows SGCP being enabled and the IP address of the call agent being specified:

```
sgcp
sgcp call-agent 209.165.200.225
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp graceful-shutdown

To block all new calls and gracefully terminate all existing calls (wait for the caller to end the call), use the **sgcp graceful-shutdown** command in global configuration mode. To unblock all calls and allow new calls to go through, use the **no** form of this command.

sgcp graceful-shutdown

no sgcp graceful-shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Once you issue this command, all requests for new connections (CreateConnection requests) are denied. All existing calls are maintained until users terminate them, or until you enter the **no sgcp** command. When the last active call is terminated, the SGCP daemon is terminated, and all resources allocated to it are released.

Examples

The following example shows all new calls being blocked and existing calls being terminated:

```
sgcp graceful-shutdown
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.

Command	Description
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp max-waiting-delay

To set the Simple Gateway Control Protocol (SGCP) maximum waiting delay to prevent restart avalanches, use the **sgcp max-waiting-delay** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp max-waiting-delay *delay*

no sgcp max-waiting-delay *delay*

Syntax Description

delay	Sets the maximum waiting delay (MWD) value in milliseconds. The valid range is from 0 to 600,000. The default is 3000.

Defaults

3,000 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only, and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Examples

The following example shows the maximum wait delay value set to 40 milliseconds:

```
sgcp max-waiting-delay 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp modem passthru

To enable Simple Gateway Control Protocol (SGCP) modem or fax pass-through, use the **sgcp modem passthru** command in global configuration mode. To disable SGCP modem or fax pass-through, use the **no** form of this command.

sgcp modem passthru {**ca** | **cisco** | **nse**}

no sgcp modem passthru {**ca** | **cisco** | **nse**}

Syntax Description

ca	Uses the call agent controlled modem upspeed method violation message.
cisco	Uses a Cisco-proprietary upspeed method based on the protocol.
nse	Uses the NSE-based modem upspeed method.

Defaults

SGCP modem or fax pass-through is disabled by default.

Command Modes

Global configuration.

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

You can use this command for fax pass-through because the answer tone can come from either modem or fax transmissions. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions.

If you use the **nse** option, you must also configure the **sgcp tse payload** command.

Examples

The following example shows SGCP modem pass-through configured using the call agent upspeed method:

```
sgcp modem passthru ca
```

The following example shows SGCP modem pass-through configured using the proprietary Cisco upspeed method:

```
sgcp modem passthru cisco
```

The following example shows SGCP modem pass-through configured using the NSE-based modem upspeed:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp quarantine-buffer disable

To disable the Simple Gateway Control Protocol (SGCP) quarantine buffer, use the **sgcp quarantine-buffer disable** command in global configuration mode. To reenable the SGCP quarantine buffer, use the **no** form of this command.

sgcp quarantine-buffer disable

no sgcp quarantine-buffer disable

Syntax Description

This command has no arguments or keywords.

Defaults

The SGCP quarantine buffer is enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

The SGCP quarantine buffer is the mechanism for buffering the SGCP events between two RQNT messages.

Examples

The following example shows the SGCP quarantine buffer being disabled:

```
sgcp quarantine-buffer disable
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.

Command	Description
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp request retries

To specify the number of times to retry sending “notify” and “delete” messages to the Simple Gateway Control Protocol (SGCP) call agent, use the **sgcp request retries** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp request retries *count*

no sgcp request retries

Syntax Description

count	Specifies the number of times a “notify” and “delete” message is retransmitted to the SGCP call agent before it is dropped. The valid range is from 1 to 100. The default is 3.

Defaults

The default for the number of times a “notify” and “delete” message is retransmitted to the SGCP call agent before it is dropped is 3

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

The actual retry count may be different from the value you enter for this command. The retry count is also limited by the call agent. If there is no response from the call agent after 30 seconds, the gateway will not retry anymore, even though the number set using the **sgcp request retries** command has not been reached.

The router will stop sending retries after 30 seconds, regardless of the setting for this command.

Examples

The following example shows the system configured to send the **sgcp** command 10 times before dropping the request:

```
sgcp request retries 10
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp request timeout

To specify how long the system should wait for a response to a request, use the **sgcp request timeout** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp request timeout *timeout*

no sgcp request timeout

Syntax Description

timeout	Specifies the number of milliseconds to wait for a response to a request. Valid range is from 1 to 10,000.

Defaults

500 milliseconds

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

This command is used for “notify” and “delete” messages, which are sent to the SGCP call agent.

Examples

The following example shows the system configured to wait 40 milliseconds for a reply to a request:

```
sgcp request timeout 40
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.

Command	Description
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp restart

To trigger the router to send a Restart in Progress (RSIP) message to the Simple Gateway Control Protocol (SGCP) call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller, use the **sgcp restart** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp restart {**delay** *delay* | **notify**}

no sgcp restart {**delay** *delay* | **notify**}

Syntax Description

delay *delay*	Specifies the restart delay timer value in milliseconds. The valid range is from 0 to 600, and the default value is 0.
notify	Enables the restart notification upon the SGCP/digital interface state transition.

Defaults

Zero (0)

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

This command is used to send RSIP messages from the router to the SGCP call agent. The RSIP messages are used to synchronize the router and the call agent. RSIP messages are also sent when the **sgcp** command is entered to enable the SGCP daemon.

You must enter the **notify** option to enable RSIP messages to be sent.

Examples

The following example shows the system configured to wait 40 milliseconds before restarting SGCP:

```
sgcp restart delay 40
```

The following example shows the system configured to send an RSIP notification to the SGCP call agent when the T1 controller state changes:

```
sgcp restart notify
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp retransmit timer

To configure the Simple Gateway Control Protocol (SGCP) retransmission timer to use a random algorithm, use the **sgcp retransmit timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp retransmit timer {**random**}

no sgcp retransmit timer {**random**}

Syntax Description

random	Enables the SGCP retransmission timer to use a random algorithm.

Defaults

The SGCP retransmission timer does not use the random algorithm.

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 3600 and Cisco MC3810 multiservice concentrator in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Use this command to enable the random algorithm component of the retransmission timer. For example, if the retransmission timer is set to 200 milliseconds, the first retransmission timer is 200 milliseconds, but the second retransmission timer picks up a timer value randomly between either 200 or 400. The third retransmission timer picks up a timer value randomly of 200, 400, or 800 as shown below:

- First retransmission timer: 200
- Second retransmission timer: 200 or 400
- Third retransmission timer: 200, 400, or 800
- Fourth retransmission timer: 200, 400, 800, or 1600
- Fifth retransmission timer: 200, 400, 800, 1600, or 3200 and so on.

After 30 seconds, the retransmission timer no longer retries.

Examples

The following example shows the retransmission timer set to use the random algorithm:

```
sgcp retransmit timer random
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp timer	Configures how the gateway detects the RTP stream host.
sgcp tse payload	Enables Inband Tse for fax/modem operation.

sgcp timer

To configure how the gateway detects the Real-Time Transport Protocol (RTP) stream lost, use the **sgcp timer** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}

no sgcp timer {**receive-rtcp** *timer* | **rtp-nse** *timer*}

Syntax Description

receive-rtcp *timer*	Sets the multiples of the RTP Control Protocol (RTCP) transmission interval in milliseconds. The valid range is from 1 to 100, and the default is 5.
rtp-nse *timer*	Sets the multiples of the RTP named signaling event (NSE) timeout in milliseconds. The valid range is from 100 to 3000, and the default is 200.

Defaults

Default for **receive-rtcp** *timer* is 5.

Default for **rtp-nse** *timer* is 200.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

The RTP NSE timer is used for proxy ringing (the ringback tone is provided at the originating gateway).

Examples

The following example shows the **receive-rtcp** *timer* set to 100 milliseconds:

```
sgcp timer receive-rtcp 100
```

The following example shows the **rtp-nse** *timer* set to 1000 milliseconds:

```
sgcp timer rtp-nse 1000
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending "notify" and "delete" messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.
sgcp tse payload	Enables Inband TSE for fax/modem operation.

sgcp tse payload

To enable Inband Telephony Signaling Events (TSE) for fax and modem operation, use the **sgcp tse payload** command in global configuration mode. To restore the default value, use the **no** form of this command.

sgcp tse payload *type*

no sgcp tse payload *type*

Syntax Description

type	Sets the TSE payload type. The valid range is from 96 to 119. The default is 0, meaning that the command is disabled.

Defaults

Zero (0)

Command Modes

Global configuration

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco MC3810 multiservice concentrator and Cisco 3600 series routers (except the Cisco 3620) in a private release that was not generally available.
12.1(2)T	This command was integrated into 12.1(2)T and was generally available on the Cisco 3600 series router and the Cisco MC3810 multiservice concentrator

Usage Guidelines

Because this command is disabled by default, you must specify a TSE payload type.

If you configure the **sgcp modem passthru** command to the **nse** value, then you must configure this command.

Examples

The following example shows the Simple Gateway Control Protocol (SGCP) modem pass-through set using the NSE-based modem upspeed and the Inband Telephony Signaling Events payload value set to 110:

```
sgcp modem passthru nse
sgcp tse payload 110
```

Related Commands

Command	Description
sgcp	Starts and allocates resources for the SGCP daemon.
sgcp call-agent	Defines the IP address of the default SGCP call agent.
sgcp graceful-shutdown	Gracefully terminates all SGCP activity.

Command	Description
sgcp max-waiting-delay	Sets the SGCP maximum waiting delay to prevent restart avalanches.
sgcp modem passthru	Enables SGCP modem or fax pass-through.
sgcp quarantine-buffer disable	Disables the SGCP quarantine buffer.
sgcp request retries	Specifies the number of times to retry sending “notify” and “delete” messages to the SGCP call agent.
sgcp request timeout	Specifies how long the system should wait for a response to a request.
sgcp restart	Triggers the router to send an RSIP message to the SGCP call agent indicating that the T1 controller is up or down so that the call agent can synchronize with the T1 controller.
sgcp retransmit timer	Configures the SGCP retransmission timer to use a random algorithm method.up or down so that the call agent can synchronize
sgcp timer	Configures how the gateway detects the RTP stream host.

show aal2 profile

To display the ATM adaptation layer 2 (AAL2) profiles configured on the system, use the **show aal2 profile** command in privileged EXEC mode.

show aal2 profile all | {**itut** *profile-number* | **custom** *profile-number* | **atmf** *profile-number*}

Syntax Description

all	Displays International Telecommunication Union Telecommunication Standardization Sector (ITU-T), ATM Forum, and custom AAL2 profiles configured on the system.
itut	Displays ITU-T profiles configured on the system.
profile-number	Specifies the profile number of the AAL2 profile to display. The available choices are as follows: For ITU-T: • 1 = G.711 u-law • 2 = G.711 u-law with silence insertion descriptor (SID) • 7 = G.711 u-law and G.729ar8 For ATMF: None. ATMF is not supported. For custom: • 100 = G.711 u-law and G.726r32 • 110 = G.711 u-law, G.726r32, and G.729ar8
custom	Displays custom profiles configured on the system.
atmf	Displays ATM Forum profiles configured on the system.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)XA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

This command applies to AAL2 Voice over ATM (VoATM) applications on the Cisco MC3810 multiservice concentrator.

Use the **show aal2 profile** EXEC command to display the AAL2 profiles configured in the system.

Examples

The following is sample output from the **show aal2 profile** command for displaying all the profiles configured in the system:

```
Router# show aal2 profile all
```

```
Printing all the Profiles in the system

Profile Type: ITUT Profile Number: 1 SID Support: 0
Red enable: 1 Num entries: 1
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15

Profile Type: ITUT Profile Number: 2 SID Support: 1
Red enable: 1 Num entries: 1
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15

Profile Type: custom Profile Number: 100 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15

Profile Type: ITUT Profile Number: 7 SID Support: 1
Red enable: 1 Num entries: 2
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 15
Coding type: g729ar8 Packet length: 10 UUI min: 0 UUI max: 15

Profile Type: custom Profile Number: 110 SID Support: 1
Red enable: 1 Num entries: 3
Coding type: g711ulaw Packet length: 40 UUI min: 0 UUI max: 7
Coding type: g726r32 Packet length: 40 UUI min: 8 UUI max: 15
Coding type: g729ar8 Packet length: 30 UUI min: 8 UUI max: 15
```

Table 26 provides an alphabetical listing of the fields in this output and a description of each field.

Table 26 show aal2 profile Field Descriptions

Field	Description
Profile Type	Category of codec types configured on DSP. Possible types are ITU-T, ATMF, and custom.
ITUT Profile Number	Predefined combination of one or more codec types configured for a digital signal processor (DSP).
SID Support	Silence insertion descriptor.
Red enable	Redundancy enable for type3 packets.
Num entries	Number of profile elements.
Coding type	Voice compression algorithm.
Packet length	Sample size.
UUI min	Minimum sequence number on the voice packets.
UUI max	Maximum sequence number on the voice packets.

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show atm video-voice address

To display the network service access point (NSAP) address for the ATM interface, enter the **show atm video-voice address** command in privileged EXEC mode.

show atm video-voice address

Syntax Description

This command has no keywords or arguments.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)T	Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Enter this command to review ATM interface NSAP addresses that have been assigned with the **atm video aesa** command and to ensure that ATM management is confirmed for those addresses.

Examples

On a Cisco MC3810 multiservice concentrator, the following example displays ATM interface NSAP addresses:

```
Router# show atm video-voice address

nsap address                                     type         ilmi status
47.0091810000000002F26D4901.00107B4832E1.FE   VOICE_AAL5   Confirmed
47.0091810000000002F26D4901.00107B4832E1.C8   VIDEO_AAL1   Confirmed
```

Related Commands

Command	Description
codec aal2-profile	Sets the codec profile for a DSP on a per-call basis.

show backhaul-session-manager group

To display status, statistics, or configuration information for all available session-groups, use the **show backhaul-session-manager group** command in privileged EXEC mode.

show backhaul-session-manager group { status | stats | cfg } { all | name *group-name* **}**

Syntax Description

status	Displays status information for session-groups.
stats	Displays statistics for session-groups.
cfg	Displays configuration information for session-groups.
all	Displays information for all available session-groups.
name *group-name*	Displays information for a specific session-group. The *group-name* argument specifies the name of the session-group.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

The following displays statistics for all session-groups:

```
Router# show backhaul-session-manager group stats all
Session-Group grp1 statistics
   Successful Fail-Overs      :0
   Un-Successful Fail-Over attempts:0
   Active Pkts receive count  :0
   Standby Pkts receive count :0
   Total PDUs dispatch err    :0
```

The following displays the current configuration for all session-groups:

```
Router# show backhaul-session-manager group cfg all
Session-Group
   Group Name :grp1
   Set Name   :set1
   Sessions   :3
    Dest:10.5.0.3 8304  Local:10.1.2.15 8304  Priority:0
    Dest:10.5.0.3 8300  Local:10.1.2.15 8300  Priority:2
    Dest:10.5.0.3 8303  Local:10.1.2.15 8303  Priority:2
    RUDP Options
      timer cumulative ack :100
      timer keepalive      :1000
      timer retransmit     :300
      timer transfer state :2000
      receive max          :32
```

```
cumulative ack max   :3
retrans max          :2
out-of-sequence max  :3
auto-reset max       :5
```

The following displays the current status of all session-groups. This group named grp1 belongs to the set named set1.

The Status will be either Group-OutOfService (no session in the group has been established) or Group-Inservice (at least one session in the group has been established).

The Status(use) will be either Group-Standby (the VSC connected to the other end of this group will go into standby mode), Group-Active (the VSC connected to the other end of this group will be the active VSC), or Group-None (the VSC has not declared its intent yet).

```
Router# show backhaul-session-manager group status all
Session-Group
Group Name   :grp1
   Set Name     :set1
   Status       :Group-OutOfService
   Status (use) :Group-None
```

Related Commands

Command	Description
show backhaul-session-manager session	Displays status, statistics, or configuration of sessions.
show backhaul-session-manager set	Displays session-groups associated with a specific or all session-sets.

show backhaul-session-manager session

To display various information for about a session or sessions, use the **show backhaul-session-manager session** command in privileged EXEC mode.

show backhaul-session-manager session { all | ip *ip_address* **}**

Syntax Description

all	All available sessions.
ip *ip_address*	The IP address of the local or remote session.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To display information for all available sessions, see the following example.

The State will be OPEN (the connection is established), OPEN_WAIT (the connection is awaiting establishment), OPEN_XFER (session failover is in progress for this session, which is a transient state), or CLOSE (this session is down, also a transient state). The session will move to OPEN_WAIT after waiting a fixed amount of time.

The Use-status field indicates whether PRI signaling traffic is currently being transported over this session . The field will be either OOS (this session is not being used to transport signaling traffic) or IS (this session is being used currently to transport all PRI signaling traffic). OOS does not indicate if the connection is established and IS indicates that the connection is established.

```
Router# show backhaul-session-manager session all

Session information --
Session-id:35
  Group:grp1  /*this session belongs to the group named 'grp1' */
Configuration:
     Local:10.1.2.15      , port:8303
    Remote:10.5.0.3       , port:8303
  Priority:2
  RUDP Option:Client, Conn Id:0x2
State:
  Status:OPEN_WAIT, Use-status:OOS,  /*see explanation below */
Statistics:
  # of resets:0
  # of auto_resets 0
  # of unexpected RUDP transitions (total) 0
  # of unexpected RUDP transitions (since last reset) 0
  Receive pkts -  Total:0 , Since Last Reset:0
  Recieve failures -  Total:0 ,Since Last Reset:0
  Transmit pkts - Total:0, Since Last Reset:0
```

```
  Transmit Failures (PDU Only)
         Due to Blocking (Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  Transmit Failures (NON-PDU Only)
         Due to Blocking(Not an Error) - Total:0, Since Last Reset:0
         Due to causes other than Blocking - Total:0, Since Last
Reset:0
  RUDP statistics
         Open failures:0
         Not ready failures:0
         Conn Not Open failures:0
         Send window full  failures:0
         Resource unavailble failures:0
         Enqueue failures:0
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.
show backhaul-session-manager set	Displays session-groups associated with a specified or all session-sets.

show backhaul-session-manager set

To display session-groups associated with a specified session-set or all session-sets, use the **show backhaul-session-manager set** command in privileged EXEC mode.

show backhaul-session-manager set { all | name *session-set-name* **}**

Syntax Description

all	All available session-sets.
name *session-set-name*	A specified session-set.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Examples

To show session groups associated with all session-sets, see the following example:

```
Router# show backhaul-session-manager set all
```

Related Commands

Command	Description
show backhaul-session-manager group	Displays status, statistics, or configuration of a specified or all session-groups.
show backhaul-session-manager session	Displays status, statistics, or configuration of a session or all sessions.

show call active

To display active call information for voice calls or fax transmissions in progress, use the **show call active** command in user EXEC or privileged EXEC mode.

show call active {**voice** | **fax**}[**brief**]

Syntax Description

voice	Specifies that information be displayed for all active voice calls.
fax	Specifies that information be displayed for all active fax calls.
brief	(Optional) Displays a truncated version of the active call information.

Defaults

No default behavior or values.

Command Modes

User EXEC or
Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 2600 series and 3600 series.
12.0(3)XG	Support for VoFR was added.
12.0(4)XJ	This command was modified for store-and-forward fax on the Cisco AS5300 universal access server.
12.0(4)T	This command was first supported on the Cisco 7200 series.
12.0(7)XK	This command was first supported on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS Release 12.1(2)T.
12.1(3)T	This command was modified for Modem Passthrough over VoIP on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **show call active** command to display the contents of the active call table. This command displays information about call times, dial peers, connections, quality of service, and other status and statistical information. If you use the **voice** keyword, information is displayed about all voice calls currently connected through the router or access server. If you use the **fax** keyword, information is displayed about all fax calls currently connected.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

See Table 19 for a listing of the information types associated with this command.

Examples

The following is sample output from the **show call active voice** command:

```
Router# show call active voice

GENERIC:
SetupTime=104443 ms
Index=1
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
ConnectTime=104964
CallDuration=00:02:43
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=2
TransmitPackets=15720
TransmitBytes=2362904
ReceivePackets=15670
ReceiveBytes=2737904
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
TxDuration=155310 ms
VoiceTxDuration=155310 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
OutSignalLevel=-13
InSignalLevel=-22
InfoActivity=2
ERLLevel=27
SessionTarget=
ImgPages=0
 GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
ConnectTime=104964
CallDuration=00:02:47
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=2
TransmitPackets=16026
TransmitBytes=2608248
ReceivePackets=16075
ReceiveBytes=2609164
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
RemoteIPAddress=1.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
```

```
SessionTarget=ipv4:1.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
SignalingType=cas

Modem passthrough signaling method is nse:
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 157sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec
```

The following is sample output from the **show call active voice brief** command:

```
Router# show call active voice brief

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes>
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
 MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
 Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

3    : 104443hs.1 +521 pid:100 Answer 50110 active
 dur 00:03:28 tx:20151/3036404 rx:20102/3517936
 Tele 0:D:1: tx:199630/199630/0ms g711ulaw noise:-75 acom:11  i/0:-22/-13 dBm

3    : 104648hs.1 +316 pid:2 Originate 55240 active
 dur 00:03:28 tx:20102/3276712 rx:20151/3277628
 IP 1.14.82.14:18202 rtt:3ms pl:40/0ms lost:0/0/0 delay:67/67/67ms g729r8
 MODEMPASS nse buf:0/0 loss 0% 0/0  last 195s dur:0/0s
```

The following is sample output from the **show call active fax** command:

```
Router# show call active fax

GENERIC:
SetupTime=22021 ms
Index=1
PeerAddress=wook song
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
ConnectTime=24284
```

```
CallState=4
CallOrigin=2
ChargedUnits=0
InfoType=10
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
RemoteIPAddress=0.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None

GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
ConnectTime=24284
CallState=4
CallOrigin=1
ChargedUnits=0
InfoType=10
TransmitPackets=5
TransmitBytes=6513
ReceivePackets=0
ReceiveBytes=0

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
TxDuration=24010 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
OutSignalLevel=0
InSignalLevel=0
InfoActivity=0
ERLLevel=-1
SessionTarget=
ImgPages=0
```

The following is sample output from the **show call active fax brief** command:

```
Router# show call active fax brief

<ID>: <start>hs.<index> +<connect> pid:<peer_id> <dir> <addr> <state> \
  tx:<packets>/<bytes> rx:<packets>/<bytes> <state>
IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
```

```
Tele <int>: tx:<tot>/<v>/<fax>ms <codec> noise:<l> acom:<l> i/o:<l>/<l> dBm

1    : 22021hs.1 +2263 pid:0 Answer wook song active
tx:0/0 rx:0/41190
IP 0.0.0.0 AcceptedMime:2 DiscardedMime:1

1    : 23193hs.1 +1091 pid:3469 Originate 527.... active
tx:10/13838 rx:0/0
Tele : tx:31200/10910/20290ms  noise:-1 acom:-1  i/0:0/0 dBm
```

Table 27 provides an alphabetical listing of the fields displayed in the output from the **show call active** command and a description of each field.

Table 27 show call active Field Descriptions

Field	Description
ACOM Level	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.
CallDuration	Length of the call in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
CallState	Current state of the call.
ChargedUnits	Total number of charging units that apply to this peer since system startup. The unit of measure for this field is hundredths of second.
CodecBytes	Payload size in bytes for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionId	Global call identifier for this gateway call.
ConnectTime	Time at which the call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet-loss events.
Corrected packet-loss Events	Total number of packet loss events that were corrected using the RFC 2198 method.
Dial-Peer	Tag of the dial peer sending this call.
ERLLevel	Current Echo Return Loss (ERL) level for this call.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from available redundancy parameters because voice data was lost or not received in time from the voice gateway for this call.

Table 27 show call active Field Descriptions (continued)

Field	Description
GapFillWithPrediction	Duration of the voice signal played out with signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call. Examples of such pullout are frame-eraser or frame-concealment strategies in G.729 and G.723.1 compression algorithms.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
HiWaterPlayoutDelay	High-water mark Voice Playout FIFO Delay during this call.
Index	Dial peer identification number.
InfoActivity	Active information transfer activity state for this call.
InfoType	Information type for this call, for example, voice or fax.
InSignalLevel	Active input signal level from the telephony interface used by this call.
Last Buffer Drain/Fill Event	Time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical interface for this call.
LoWaterPlayoutDelay	Low water mark Voice Playout FIFO Delay during this call.
Modem passthrough signaling method in use	Indicates that this is a modem pass-through call and that named signaling events (NSEs)—also called *telephone-events* in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Active noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
OutSignalLevel	Active output signal level to the telephony interface used by this call.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer table entry to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress when this call is connected.
Percent Packet Loss	Total percent packet loss.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for the VoIP call.
RemoteUDPPort	Remote system UDP listener port to which voice packets are sent.

Table 27 show call active Field Descriptions (continued)

Field	Description
RoundTripDelay	Voice packet round trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected RSVP quality of service (QoS) for this call.
SessionProtocol	Session protocol used for an Internet call between the local and remote routers through the IP backbone.
SessionTarget	Session target of the peer used for this call.
SetupTime	Value of the system UpTime when the call associated with this entry was started.
SignalingType	Signaling type for this call; for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	Duration of transmit path open from this peer to the voice gateway for this call.
VAD	Whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

Related Commands

Command	Description
show call history	Displays the call history table.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

show call application voice

To define the names of the audio files that the interactive voice response (IVR) script will play, the operation of the abort keys, the prompts that are used, and caller interaction, use the **show call application voice** command in EXEC mode.

show call application voice [*name* | **summary**]

Syntax Description

name	(Optional) The name of the desired IVR application.
summary	(Optional) Displays a one-line summary. If the command is entered without the **summary** keyword, a complete detailed description is displayed of the application.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2500 series and Cisco 3600 series routers and the Cisco AS5300 universal access server.

Usage Guidelines

If the name of a specific application is entered, it will give information about that application.

If the **summary** keyword is entered, a one-line summary will be displayed about each application.

If the command is entered without the **summary**, a detailed description of the entered IVR application is displayed.

Examples

This example shows the output for the clid_authen_collect IVR script:

```
Router# show call application voice clid_authen_collect

Application clid_authen_collect has 10 states with 0 calls active
 State start has 1 actions and 5 events
    Do Action IVR_ACT_AUTHENTICATE. accountName=ani, pinName=dnis
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_CALL_SETUP_IND do action IVR_ACT_CALL_SETUP_ACK
          and goto state start
    If Event IVR_EV_AAA_SUCCESS goto state collect_dest
    If Event IVR_EV_AAA_FAIL goto state get_account
 State end has 1 actions and 3 events
    Do Action IVR_ACT_END.
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_CALL_DISCONNECT_DONE do action IVR_ACT_CALL_DESTROY
```

```
          and do nothing
State get_account has 4 actions and 7 events
    Do Action IVR_ACT_PLAY.
            URL: flash:enter_account.au
            allowInt=1, pContent=0x60E4C564
    Do Action IVR_ACT_ABORT_KEY. abortKey=*
    Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
    Do Action IVR_ACT_COLLECT_PATTERN. Pattern account is .+
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_PAT_COL_SUCCESS goto state get_pin
            patName=account
    If Event IVR_EV_ABORT goto state get_account
    If Event IVR_EV_PLAY_COMPLETE do nothing
    If Event IVR_EV_TIMEOUT goto state get_account count=0
    If Event IVR_EV_PAT_COL_FAIL goto state get_account
 State get_pin has 4 actions and 7 events
    Do Action IVR_ACT_PLAY.
            URL: flash:enter_pin.au
            allowInt=1, pContent=0x0
    Do Action IVR_ACT_ABORT_KEY. abortKey=*
    Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
    Do Action IVR_ACT_COLLECT_PATTERN. Pattern pin is .+
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_PAT_COL_SUCCESS goto state authenticate
            patName=pin
    If Event IVR_EV_PLAY_COMPLETE do nothing
    If Event IVR_EV_ABORT goto state get_account
    If Event IVR_EV_TIMEOUT goto state get_pin count=0
    If Event IVR_EV_PAT_COL_FAIL goto state get_pin
 State authenticate has 1 actions and 5 events
    Do Action IVR_ACT_AUTHENTICATE. accountName=account, pinName=pin
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_AAA_SUCCESS goto state collect_dest
    If Event IVR_EV_TIMEOUT do nothing count=0
    If Event IVR_EV_AAA_FAIL goto state authenticate_fail
 State collect_dest has 4 actions and 8 events
    Do Action IVR_ACT_PLAY.
            URL: flash:enter_destination.au
            allowInt=1, pContent=0x0
    Do Action IVR_ACT_ABORT_KEY. abortKey=*
    Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
    Do Action IVR_ACT_COLLECT_DIALPLAN.
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_PLAY_COMPLETE do nothing
    If Event IVR_EV_ABORT goto state collect_dest
    If Event IVR_EV_TIMEOUT goto state collect_dest count=0
    If Event IVR_EV_DIAL_COL_SUCCESS goto state place_call
    If Event IVR_EV_DIAL_COL_FAIL goto state collect_dest
    If Event IVR_EV_TIMEOUT goto state collect_dest count=0
 State place_call has 1 actions and 4 events
    Do Action IVR_ACT_PLACE_CALL.
            destination= called=
            calling=      account=
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_CALL_UP goto state active
    If Event IVR_EV_CALL_FAIL goto state place_fail
 State active has 0 actions and 2 events
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
```

```
 State authenticate_fail has 1 actions and 2 events
    Do Action IVR_ACT_PLAY.
            URL: flash:auth_failed.au
            allowInt=0, pContent=0x0
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
 State place_fail has 1 actions and 2 events
    Do Action IVR_ACT_PLAY_FAILURE_TONE.
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing

Router# show call application voice clid_authen_collect

Application clid_authen_collect has 10 states with 0 calls active
 State start has 1 actions and 5 events
    Do Action IVR_ACT_AUTHENTICATE. accountName=ani, pinName=dnis
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_CALL_SETUP_IND do action IVR_ACT_CALL_SETUP_ACK
          and goto state start
    If Event IVR_EV_AAA_SUCCESS goto state collect_dest
    If Event IVR_EV_AAA_FAIL goto state get_account
 State end has 1 actions and 3 events
    Do Action IVR_ACT_END.
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_CALL_DISCONNECT_DONE do action IVR_ACT_CALL_DESTROY
          and do nothing
 State get_account has 4 actions and 7 events
    Do Action IVR_ACT_PLAY.
            URL: flash:enter_account.au
            allowInt=1, pContent=0x60E4C564
    Do Action IVR_ACT_ABORT_KEY. abortKey=*
    Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
    Do Action IVR_ACT_COLLECT_PATTERN. Pattern account is .+
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_PAT_COL_SUCCESS goto state get_pin
            patName=account
    If Event IVR_EV_ABORT goto state get_account
    If Event IVR_EV_PLAY_COMPLETE do nothing
    If Event IVR_EV_TIMEOUT goto state get_account count=0
    If Event IVR_EV_PAT_COL_FAIL goto state get_account
 State get_pin has 4 actions and 7 events
    Do Action IVR_ACT_PLAY.
            URL: flash:enter_pin.au
            allowInt=1, pContent=0x0
    Do Action IVR_ACT_ABORT_KEY. abortKey=*
    Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
    Do Action IVR_ACT_COLLECT_PATTERN. Pattern pin is .+
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_PAT_COL_SUCCESS goto state authenticate
            patName=pin
    If Event IVR_EV_PLAY_COMPLETE do nothing
    If Event IVR_EV_ABORT goto state get_account
    If Event IVR_EV_TIMEOUT goto state get_pin count=0
    If Event IVR_EV_PAT_COL_FAIL goto state get_pin
 State authenticate has 1 actions and 5 events
    Do Action IVR_ACT_AUTHENTICATE. accountName=account, pinName=pin
    If Event IVR_EV_DEFAULT goto state end
    If Event IVR_EV_CALL_DIGIT do nothing
    If Event IVR_EV_AAA_SUCCESS goto state collect_dest
    If Event IVR_EV_TIMEOUT do nothing count=0
```

```
   If Event IVR_EV_AAA_FAIL goto state authenticate_fail
State collect_dest has 4 actions and 8 events
   Do Action IVR_ACT_PLAY.
           URL: flash:enter_destination.au
           allowInt=1, pContent=0x0
   Do Action IVR_ACT_ABORT_KEY. abortKey=*
   Do Action IVR_ACT_TERMINATION_KEY. terminationKey=#
   Do Action IVR_ACT_COLLECT_DIALPLAN.
   If Event IVR_EV_DEFAULT goto state end
   If Event IVR_EV_CALL_DIGIT do nothing
   If Event IVR_EV_PLAY_COMPLETE do nothing
   If Event IVR_EV_ABORT goto state collect_dest
   If Event IVR_EV_TIMEOUT goto state collect_dest count=0
   If Event IVR_EV_DIAL_COL_SUCCESS goto state place_call
   If Event IVR_EV_DIAL_COL_FAIL goto state collect_dest
   If Event IVR_EV_TIMEOUT goto state collect_dest count=0
State place_call has 1 actions and 4 events
   Do Action IVR_ACT_PLACE_CALL.
           destination= called=
           calling=      account=
   If Event IVR_EV_DEFAULT goto state end
   If Event IVR_EV_CALL_DIGIT do nothing
   If Event IVR_EV_CALL_UP goto state active
   If Event IVR_EV_CALL_FAIL goto state place_fail
State active has 0 actions and 2 events
   If Event IVR_EV_DEFAULT goto state end
   If Event IVR_EV_CALL_DIGIT do nothing
State authenticate_fail has 1 actions and 2 events
   Do Action IVR_ACT_PLAY.
           URL: flash:auth_failed.au
           allowInt=0, pContent=0x0
   If Event IVR_EV_DEFAULT goto state end
   If Event IVR_EV_CALL_DIGIT do nothing
State place_fail has 1 actions and 2 events
   Do Action IVR_ACT_PLAY_FAILURE_TONE.
   If Event IVR_EV_DEFAULT goto state end
   If Event IVR_EV_CALL_DIGIT do nothing
```

Related Commands

Command	Description
call application voice	Defines the name to be used for an application and indicates the location of the appropriate IVR script to be used with this application.
call application voice load	Reloads the designated TCL script.

show call fallback cache

To see the current Calculated Planning Impairment Factor (ICPIF) estimates for all IP addresses in cache, use the **show call fallback cache** command in EXEC mode.

show call fallback cache [*ip-address*]

Syntax Description

ip-address	(Optional) Specifies a specific IP address.

Defaults

This command is not configured by default.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

To clear all entries in the cache, use the **clear call fallback cache** command.

Examples

The following example displays output from the **show call fallback cache** command:

```
Router# show call fallback cache

Probe   IP Address      Codec   Delay   Loss    ICPIF   Reject  Accept
-----   ----------      -----   -----   ----    -----   ------  ------
1       1.1.1.4         g729r8  40      00       0       9
2       122.24.56.25    g729r8  14810      5       1       4

2 active probes

Field                       Description
-------                     ------------
Probe                       Probe number
IP Address                  IP Address to which the probe is sent
Codec                       Codec Type of the probe
Delay                       Delay in milliseconds that the probe incurred
Loss                        Loss in % that the probe incurred
ICPIF                       Computed ICPIF value for the probe
Reject                      Number of times that calls of Codec Type <Codec>
                            were rejected to the IP Address
Accept                      Number of times that calls of Codec Type <Codec>
                            were accepted to the IP Address
active probes               Number of destinations being probed
```

```
Router# show call fallback cache 10.14.115.53

Probe    IP Address       Codec            ICPIF    Reject   Accept
-----    ----------       -----            -----    ------   ------
1        10.14.115.53      g729r8           0        0        2

1 active probes
```

Related Commands

Command	Description
show call fallback stats	Displays the call fallback statistics.

show call fallback config

To display the call fallback configuration, use the **show call fallback config** command in EXEC mode.

show call fallback config

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not configured by default.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Examples

The following example displays output from the **show call fallback config** command:

```
Router# show call fallback config

VoIP fallback config:
Fallback is ON
Using ICPIF threshold:
        ICPIF value timeout:20 seconds
        ICPIF threshold:20
Number of packets in a probe:20
IP precedence of probe packets:2
Fallback cache size:2 entries
Fallback cache timeout:240 seconds
Instantaneous value weight:65
MD5 Keychain:secret
```

Related Commands

Command	Description
call fallback monitor	Enables the monitoring of destinations without fallback to alternate dial peers.
show voice trunk-conditioning signaling	Enables fallback to alternate dial peers in case of network congestion.

show call fallback stats

To display the call fallback statistics, use the **show call fallback stats** command in EXEC mode.

show call fallback stats

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not configured by default.

Command Modes

EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

To remove all values, use the **clear call fallback stats** command.

Examples

The following example displays output from the **show call fallback stats** command:

```
Router# show call fallback stats

VOIP Fallback Stats:
Total accepted calls:3
Total rejected calls:1
Total cache overflows:1

Field                      Description
-------                    ------------
Total accepted calls       Number of times that calls were successful over IP.
Total rejected calls       Number of times that calls were rejected over IP.
Total cache overflows      Number of times that the fallback cache overflowed and requied
pruning.
```

Related Commands

Command	Description
clear call fallback stats	Clears the call fallback statistics.
show call fallback cache	Displays the current ICPIF estimates for all IP addresses in the cache.

show call history

To display the call history table for voice calls or fax transmissions, use the **show call history** command in user EXEC or privileged EXEC mode.

show call history {**voice** | **fax**}[**last** *number* | **brief**]

Syntax Description

voice	Specifies that call history information be displayed for voice calls.
fax	Specifies that call history information be displayed for fax calls.
last *number*	(Optional) Displays the last calls connected, where the number of calls that appear is defined by the *number* argument. Valid values are from 1 to 100.
brief	(Optional) Displays a truncated version of the call history table.

Defaults

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series.
12.0(3)XG	Support for Voice over Frame Relay (VoFR) was added on the Cisco 2600 and Cisco 3600 series.
12.0(4)XJ	This command was modified for store-and-forward fax.
12.0(4)T	The **brief** keyword was added and the command was first supported on the Cisco 7200 series.
12.0(7)XK	Support for the **brief** keyword was added on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS 12.1(2)T.

Usage Guidelines

The **show call history** command displays a call history table containing a list of voice or fax calls connected through the router in descending time order. The maximum number of calls contained in the table can be set to a number between 0 and 500 using the **dial-control-mib** command in global configuration mode. The default maximum number of table entries is 50. Each call record is aged out of the table after a configurable number of minutes has elapsed, also specified by the **dial-control-mib** command. The default timer value is 15 minutes.

You can display subsets of the call history table by using specific keywords. To display the last calls connected through this router, use the keyword **last**, and define the number of calls to be displayed with the *number* argument.

To display a truncated version of the call history table, use the **brief** keyword.

When using the **fax** keyword, this command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following is sample output from the **show call history voice** command:

```
Router# show call history voice

GENERIC:
SetupTime=104648 ms
Index=1
PeerAddress=55240
PeerSubAddress=
PeerId=2
PeerIfIndex=105
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143329
CallDuration=00:06:23
CallOrigin=1
ChargedUnits=0
InfoType=speech
TransmitPackets=37668
TransmitBytes=6157536
ReceivePackets=37717
ReceiveBytes=6158452
VOIP:
ConnectionId[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
RemoteIPAddress=1.14.82.14
RemoteUDPPort=18202
RoundTripDelay=2 ms
SelectedQoS=best-effort
tx_DtmfRelay=inband-voice
FastConnect=TRUE

SessionProtocol=cisco
SessionTarget=ipv4:1.14.82.14
OnTimeRvPlayout=40
GapFillWithSilence=0 ms
GapFillWithPrediction=0 ms
GapFillWithInterpolation=0 ms
GapFillWithRedundancy=0 ms
HiWaterPlayoutDelay=67 ms
LoWaterPlayoutDelay=67 ms
ReceiveDelay=67 ms
LostPackets=0 ms
EarlyPackets=0 ms
LatePackets=0 ms
VAD = enabled
CoderTypeRate=g729r8
CodecBytes=20
cvVoIPCallHistoryIcpif=0
SignalingType=cas

Modem passthrough signaling method is nse
Buffer Fill Events = 0
Buffer Drain Events = 0
Percent Packet Loss = 0
Consecutive-packets-lost Events = 0
```

```
Corrected packet-loss Events = 0
Last Buffer Drain/Fill Event = 373sec
Time between Buffer Drain/Fills = Min 0sec Max 0sec

GENERIC:
SetupTime=104443 ms
Index=2
PeerAddress=50110
PeerSubAddress=
PeerId=100
PeerIfIndex=104
LogicalIfIndex=10
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=104964
DisconectTime=143330
CallDuration=00:06:23
CallOrigin=2
ChargedUnits=0
InfoType=speech
TransmitPackets=37717
TransmitBytes=5706436
ReceivePackets=37668
ReceiveBytes=6609552
TELE:
ConnectionId=[0x4B091A27 0x3EDD0003 0x0 0xFEFD4]
TxDuration=375300 ms
VoiceTxDuration=375300 ms
FaxTxDuration=0 ms
CoderTypeRate=g711ulaw
NoiseLevel=-75
ACOMLevel=11
SessionTarget=
ImgPages=0
```

The following is sample output from the **show call history voice brief** command:

```
Router# show call history voice brief

<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
  dur hh:mm:ss tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
  MODEMPASS <method> buf:<fills>/<drains> loss <overall%> <multipkt>/<corrected>
   last <buf event time>s dur:<Min>/<Max>s
 FR <protocol> [int dlci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
 ATM <protocol> [int vpi/vci cid] vad:<y/n> dtmf:<y/n> seq:<y/n>
  sig:<on/off> <codec> (payload size)
 Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm
```

The following is sample output from the **show call history fax** command:

```
Router# show call history fax

GENERIC:
SetupTime=23193 ms
Index=1
PeerAddress=527....
PeerSubAddress=
PeerId=3469
PeerIfIndex=157
LogicalIfIndex=30
DisconnectCause=10
```

```
DisconnectText=normal call clearing.: Normal connection
ConnectTime=24284
DisconectTime=31288
CallOrigin=1
ChargedUnits=0
InfoType=fax
TransmitPackets=62
TransmitBytes=88047
ReceivePackets=0
ReceiveBytes=0

TELE:
ConnectionId=[0x37EC7F41 0xB0110001 0x0 0x35C34]
TxDuration=80950 ms
FaxTxDuration=10910 ms
FaxRate=14400
NoiseLevel=-1
ACOMLevel=-1
SessionTarget=
ImgPages=3

GENERIC:
SetupTime=22021 ms
Index=2
PeerAddress=wook song
PeerSubAddress=
PeerId=0
PeerIfIndex=0
LogicalIfIndex=0
DisconnectCause=10
DisconnectText=normal call clearing.
ConnectTime=24284
DisconectTime=31545
CallOrigin=2
ChargedUnits=0
InfoType=fax
TransmitPackets=0
TransmitBytes=0
ReceivePackets=0
ReceiveBytes=41190

MMOIP:
ConnectionId[0x37EC7F41 0xB0110001 0x0 0x35C34]
RemoteIPAddress=0.0.0.0
SessionProtocol=SMTP
SessionTarget=
MessageId=
AccountId=
ImgEncodingType=MH
ImgResolution=fine
AcceptedMimeTypes=2
DiscardedMimeTypes=1
Notification=None
```

The following is sample output from the **show call history fax brief** command:

```
Router# show call history fax brief

<ID>: <start>hs.<index> +<connect> +<disc> pid:<peer_id> <direction> <addr>
 tx:<packets>/<bytes> rx:<packets>/<bytes> <disc-cause>(<text>)
 IP <ip>:<udp> rtt:<time>ms pl:<play>/<gap>ms lost:<lost>/<early>/<late>
  delay:<last>/<min>/<max>ms <codec>
 Telephony <int>: tx:<tot>/<voice>/<fax>ms <codec> noise:<lvl>dBm acom:<lvl>dBm
```

```
2     : 5996450hs.25 +-1 +3802 pid:100 Answer 408
 tx:0/0 rx:0/0 1F  (T30 T1 EOM timeout)
 Telephony : tx:38020/38020/0ms g729r8 noise:0dBm acom:0dBm

2     : 5996752hs.26 +-1 +3500 pid:110 Originate uut1@linux2.allegro.com
 tx:0/0 rx:0/0 3F  (The e-mail was not sent correctly. Remote SMTP server said: 354 )
 IP 14.0.0.1 AcceptedMime:0 DiscardedMime:0

3     : 6447851hs.27 +1111 +3616 pid:310 Originate 576341.
 tx:11/14419 rx:0/0 10  (Normal connection)
 Telephony : tx:36160/11110/25050ms g729r8 noise:115dBm acom:-14dBm

3     : 6447780hs.28 +1182 +4516 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

4     : 6464816hs.29 +1050 +3555 pid:310 Originate 576341.
 tx:11/14413 rx:0/0 10  (Normal connection)
 Telephony : tx:35550/10500/25050ms g729r8 noise:115dBm acom:-14dBm

4     : 6464748hs.30 +1118 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

5     : 6507900hs.31 +1158 +2392 pid:100 Answer 4085763413
 tx:0/0 rx:3/3224 10  (Normal connection)
 Telephony : tx:23920/11580/12340ms g729r8 noise:0dBm acom:0dBm

5     : 6508152hs.32 +1727 +2140 pid:110 Originate uut1@linux2.allegro.com
 tx:0/2754 rx:0/0 3F  (service or option not available, unspecified)
 IP 14.0.0.4 AcceptedMime:0 DiscardedMime:0

6     : 6517176hs.33 +1079 +3571 pid:310 Originate 576341.
 tx:11/14447 rx:0/0 10  (Normal connection)
 Telephony : tx:35710/10790/24920ms g729r8 noise:115dBm acom:-14dBm

6     : 6517106hs.34 +1149 +4517 pid:0 Answer
 tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0

7     : 6567382hs.35 +1054 +3550 pid:310 Originate 576341.
 tx:11/14411 rx:0/0 10  (Normal connection)
 Telephony : tx:35500/10540/24960ms g729r8 noise:115dBm acom:-14dBm

7     : 6567308hs.36 +1128 +4517 pid:0 Answer
tx:0/0 rx:0/0 10  (normal call clearing.)
 IP 0.0.0.0 AcceptedMime:0 DiscardedMime:0
```

Table 28 provides an alphabetical listing of the fields displayed in the output from the **show call history** command and a description of each field.

Table 28 show call history Field Descriptions

Field	Description
ACOMLevel	Current ACOM level for this call. ACOM is the combined loss achieved by the echo canceler, which is the sum of the Echo Return Loss, Echo Return Loss Enhancement, and nonlinear processing loss for the call.
Buffer Drain Events	Total number of jitter buffer drain events.
Buffer Fill Events	Total number of jitter buffer fill events.

Table 28 show call history Field Descriptions (continued)

Field	Description
CallDuration	Length of the call, in hours, minutes, and seconds, hh:mm:ss.
CallOrigin	Call origin: answer or originate.
ChargedUnits	Total number of charging units applying to this peer since system startup. The unit of measure for this field is hundredths of a second.
CodecBytes	Payload size in bytes for the codec used.
CoderTypeRate	Negotiated coder rate. This value specifies the send rate of voice or fax compression to its associated call leg for this call.
ConnectionID	Global call identifier for the gateway call.
ConnectTime	Time at which this call was connected.
Consecutive-packets-lost Events	Total number of consecutive (two or more) packet loss events.
Corrected packet-loss Events	Total number of packet-loss events that were corrected using the RFC 2198 method.
DisconnectCause	Description explaining why this call was disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.
DisconnectTime	Time when this call was disconnected.
FaxTxDuration	Duration of fax transmission from this peer to the voice gateway for this call. You can derive the Fax Utilization Rate by dividing the FaxTxDuration value by the TxDuration value.
GapFillWithInterpolation	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding and following in time, because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithRedundancy	Duration of a voice signal played out with a signal synthesized from redundancy parameters available because voice data was lost or not received in time from the voice gateway for this call.
GapFillWithSilence	Duration of a voice signal replaced with silence because voice data was lost or not received in time for this call.
GapFillWithPrediction	Duration of a voice signal played out with a signal synthesized from parameters, or samples of data preceding in time, because voice data was lost or not received in time from the voice gateway for this call.
HiWaterPlayoutDelay	High-water mark Voice Playout FIFO Delay during this voice call.
Index	Dial peer identification number.
InfoType	Information type for this call; for example, voice or fax.
Last Buffer Drain/Fill Event	Time since the last jitter buffer drain or fill event, in seconds.
LogicalIfIndex	Index number of the logical voice port for this call.
LoWaterPlayoutDelay	Low-water mark Voice Playout FIFO Delay during this voice call.

Table 28 show call history Field Descriptions (continued)

Field	Description
Modem passthrough signaling method is nse	Indicates that this is a modem pass-through call and named signaling events (NSEs)—also called *telephone-events* in RFC 2833—are used for signaling codec upspeed. The upspeed method is the method used to dynamically change the codec type and speed to meet network conditions. This means that you might move to a faster codec when you have both voice and data calls and then slow down when there is only voice traffic.
NoiseLevel	Average noise level for this call.
OnTimeRvPlayout	Duration of voice playout from data received on time for this call. Derive the Total Voice Playout Duration for Active Voice by adding the OnTimeRvPlayout value to the GapFill values.
Percent Packet Loss	Total percent packet loss.
PeerAddress	Destination pattern or number associated with this peer.
PeerId	ID value of the peer entry table to which this call was made.
PeerIfIndex	Voice port index number for this peer. For ISDN media, this would be the index number of the B channel used for this call.
PeerSubAddress	Subaddress where this call is connected.
ReceiveBytes	Number of bytes received by the peer during this call.
ReceiveDelay	Average Playout FIFO Delay plus the Decoder Delay during this voice call.
ReceivePackets	Number of packets received by this peer during this call.
RemoteIPAddress	Remote system IP address for this call.
RemoteUDPPort	Remote system UDP listener port to which voice packets are sent.
RoundTripDelay	Voice packet round-trip delay between the local and remote systems on the IP backbone for this call.
SelectedQoS	Selected RSVP QoS for this call.
Session Protocol	Session protocol used for an Internet call between the local and remote router through the IP backbone.
Session Target	Session target of the peer used for this call.
SetUpTime	Value of the system UpTime when the call associated with this entry was started.
SignalingType	Signaling type for this call, for example, channel-associated signaling (CAS) or common-channel signaling (CCS).
Time between Buffer Drain/Fills	Minimum and maximum durations between jitter buffer drain or fill events, in seconds.
TransmitBytes	Number of bytes sent by this peer during this call.
TransmitPackets	Number of packets sent by this peer during this call.
TxDuration	Duration of the transmit path open from this peer to the voice gateway for this call.

Table 28 show call history Field Descriptions (continued)

Field	Description
VAD	Specifies whether voice activation detection (VAD) was enabled for this call.
VoiceTxDuration	Duration of voice transmission from this peer to the voice gateway for this call. Derive the Voice Utilization Rate by dividing the VoiceTxDuration value by the TxDuration value.

Related Commands

Command	Description
show call active	Displays the active call information for voice calls or fax transmissions in progress.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

show call history video record

To display information about video calls, use the **show call history video record** command in privileged EXEC mode.

show call history video record

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to review statistics about recent incoming and outgoing video calls.

Examples

On a Cisco MC3810 multiservice concentrator, the following example displays information about two video calls:

```
Router# show call history video record

CallId = 4
CalledNumber = 221
CallDuration = 39006 seconds
DisconnectText = remote hangup
SVC: call ID = 8598630
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 414, vpi = 0, vci = 158
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
CallId = 3
CalledNumber = 221
CallDuration = 557 seconds
DisconnectText = local hangup
SVC: call ID = 8598581
Remote NSAP = 47.0091810000000002F26D4901.00107B09C645.C8
Local NSAP = 47.0091810000000002F26D4901.00107B4832E1.C8
vcd = 364, vpi = 0, vci = 108
SerialPort = Serial0
VideoSlot = 1, VideoPort = 0
```

show call history voice record

To display Call Detail Record (CDR) events in the call history table, use the **show call history voice record** command in privileged EXEC mode.

show call history voice record

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Examples

The following example displays a sample of voice call history records showing a local call between two telephones attached to the same Cisco MC3810 multiservice concentrator:

```
Router# show call history voice record

ConnectionId=[0x2C7AEFDC 0x59830001 0x0 0xB0AAA3]
Media=TELE, TxDuration= 1418 ms
CallingNumber=2001
SetupTime=1157801 x 10ms
ConnectTime=1158046 x 10ms
DisconectTime=1158188 x 10ms
DisconnectText=local onhook

ConnectionId=[0x2C7AEFDC 0x59830001 0x0 0xB0AAA3]
Media=TELE, TxDuration= 1422 ms
CalledNumber=2002
SetupTime=1157802 x 10ms
ConnectTime=1158046 x 10ms
DisconectTime=1158188 x 10ms
DisconnectText=remote onhook
```

Table 29 describes the significant fields shown in the display.

Table 29 show call history voice record Field Descriptions

Field	Description
ConnectionID	Global call identifier for this voice call.
Media	Medium over which the call is carried. If the call is carried over the (telephone) access side, the entry will be TELE. If the call is carried over the voice network side, the entry will be either ATM, FR (for Frame Relay), or HDLC.
LowerIFName	Physical lower interface information. Appears only if the medium is either ATM, FR, or HDLC.
TxDuration	The length of the call. Appears only if the medium is TELE.
CalledNumber	The called number.
CallingNumber	The calling number.
SetupTime	Time the call setup started.
ConnectTime	Time the call is connected.
DisconnectTime	Time the call is disconnected.
DisconnectText	Descriptive text explaining the reason for the disconnect.

Related Commands

Command	Description
show call active voice	Displays the Voice over IP active call table.
show dial-peer voice	Displays configuration information for dial peers.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

show call resource voice stats

To display resource statistics for an H.323 gateway, use the **show call resource voice stats** command in privileged EXEC mode.

show call resource voice stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

This command displays the H.323 resources that are monitored when the **resource threshold** command is used to configure and enable resource threshold reporting.

Examples

The following example shows the resource statistics for an H.323 gateway:

```
Router# show call resource voice stats

Resource Monitor -  Dial-up Resource Statistics Information:

DSP Statistics:

Utilization: 0 percent
Total channels: 48
Inuse channels: 0
Disabled channels 0:
Pending channels: 0
Free channels: 48

DS0 Statistics:

Total channels: 0
Addressable channels: 0
Inuse channels: 0
Disabled channels: 0
Free channels: 0
```

Table 30 describes the significant fields shown in the display.

Table 30 show call resource voice stats Field Descriptions

Statistic	Definition
Total channels	Number of channels physically configured for the resource.
Addressable channels	Number of channels that can be used for a specific type of dialup service, such as H.323, which includes all the DS0 resources that have been associated with a voice plain old telephone service (POTS) dial plan profile.
Inuse channels	Number of addressable channels that are in use. This value includes all channels that either have active calls or have been reserved for testing.
Free channels	Number of addressable channels that are free.
Pending channels	Number of addressable channels that are pending in loadware download.
Disabled channels	Number of addressable channels that are physically down or that have been disabled administratively with the **shutdown** or **busyout** command.

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice threshold	Displays the threshold configuration settings and status for an H.323 gateway.

show call resource voice threshold

To display the threshold configuration settings and status for an H.323 gateway, use the **show call resource voice threshold** command in privileged EXEC mode.

show call resource voice threshold

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced on the Cisco AS5300 univeral access server.

Usage Guidelines

This command displays the H.323 resource thresholds that are configured with the **resource threshold** command.

Examples

The following example shows the resource threshold settings and status for an H.323 gateway:

```
Router# show call resource voice threshold

Resource Monitor -  Dial-up Resource Threshold Information:

DS0 Threshold:

Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: init
DSP Threshold:

Client Type: h323
High Water Mark: 70
Low Water Mark: 60
Threshold State: low_threshold_hit
```

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.
show call resource voice stats	Displays resource statistics for an H.323 gateway.

show call rsvp-sync conf

To display the configuration settings for Resource Reservation Protocol (RSVP) synchronization, use the **show call rsvp-sync conf** command in privileged EXEC mode.

show call rsvp-sync conf

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XI1	This command was introduced on the Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers, the Cisco MC3810 multiservice concentrator, and on the Cisco AS5300 and Cisco AS5800 universal access servers.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following example shows sample output from the **show call rsvp-sync conf** command:

```
Router# show call rsvp-sync conf

VoIP QoS: RSVP/Voice Signaling Synchronization config:

Overture Synchronization is ON
Reservation Timer is set to 10 seconds
```

Table 31 describes the significant fields shown in the display

Table 31 show call rsvp-sync conf Field Descriptions

Field	Description
Overture Synchronization is ON	Indicates whether RSVP synchronization is enabled.
Reservation Timer is set to xx seconds	Number of seconds for which the RSVP reservation timer is configured.

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync stats	Displays statistics for calls that attempted RSVP reservation.

show call rsvp-sync stats

To display statistics for calls that attempted Resource Reservation Protocol (RSVP) reservation, use the **show call rsvp-sync stats** command in privileged EXEC mode.

show call rsvp-sync stats

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)XI1	This command was introduced.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.

Examples

The following example shows sample output from the **show call rsvp-sync stats** command:

```
Router# show call rsvp-sync stats

VoIP QoS:Statistics Information:
Number of calls for which QoS was initiated   : 18478
Number of calls for which QoS was torn down   : 18478
Number of calls for which Reservation Success was notified : 0
Total Number of PATH Errors encountered : 0
Total Number of RESV Errors encountered : 0
Total Number of Reservation Timeouts encountered : 0
```

Table 32 describes the significant fields shown in the display.

Table 32 show call rsvp-sync stats Field Descriptions

Field	Description
Number of calls for which QoS was initiated	Number of calls for which RSVP setup was attempted.
Number of calls for which QoS was torn down	Number of calls for which an established RSVP reservation was released.
Number of calls for which Reservation Success was notified	Number of calls for which an RSVP reservation was successfully established.
Total Number of PATH Errors encountered	Number of path errors that occurred.
Total Number of RESV Errors encountered	Number of reservation errors that occurred.
Total Number of Reservation Timeouts encountered	Number of calls in which the reservation setup was not complete before the reservation timer expired.

Related Commands

Command	Description
call rsvp-sync	Enables synchronization between RSVP and the H.323 voice signaling protocol.
call rsvp-sync resv-timer	Sets the timer for RSVP reservation setup.
debug call rsvp-sync events	Displays the events that occur during RSVP synchronization.
show call rsvp-sync conf	Displays the RSVP synchronization configuration.

show cdapi

To display the Call Distributor Application Programming Interface (CDAPI), use the **show cdapi** command in privileged EXEC mode.

show cdapi

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

CDAPI is the internal application programming interface (API) that provides an interface between signaling stacks and applications.

Examples

The following is output for the **show cdapi** command:

```
Router# show cdapi

Registered CDAPI Applications/Stacks
====================================
Application TSP CDAPI Application
        Application Type(s)  Voice Facility Signaling
        Application Level    Tunnel
        Application Mode     Enbloc
Signaling Stack ISDN
        Interface Se023
Signaling Stack ISDN
        Interface Se123
Active CDAPI Calls
==================
Interface Se023
        No active calls.
Interface Se123
        Call ID = 0x39, Call Type = VOICE, Application = TSP CDAPI Application
CDAPI Message Buffers
=====================
Used Msg Buffers 0, Free Msg Buffers 1600
Used Raw Buffers 1, Free Raw Buffers 799
Used Large-Raw Buffers 0, Free Large-Raw Buffers 80
scarlatti1#
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support Q.SIG signaling.
pri-group nec-fusion	Configures your NEC PBX to support FCCS.
show rawmsg	Displays the raw messages owned by the required component.

show ces clock-select

To display the setting of the network clock for the specified port, use the **show ces clock-select** command in privileged EXEC mode.

show ces *slot*/*port* **clock-select**

Syntax Description

slot	Backplane slot number.
/*port*	Interface port number. The slash must be entered.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(2)T	This command was introduced on the Cisco 3600 series router.

Examples

The following is sample output from the **show ces clock-select** command for slot 1, port 0:

```
Router# show ces 1/0 clock-select

Priority 1 clock source:not configured
Priority 2 clock source:not configured
Priority 3 clock source:ATM1/0 UP
Priority 4 clock source:Local oscillator
Current clock source:ATM1/0, priority:3
```

Related Commands

Command	Description
clock-select	Establishes the sources and priorities of the requisite clocking signals for the OC-3/STM-1 ATM Circuit Emulation Service network module.

show connect

To display configuration information about drop-and-insert connections that have been configured on a router, enter the **show connect** command in privileged EXEC mode.

show connect {**all** | **elements** | **name** | **id** | **port** {**T1** | **E1**} *slot*/*port*}}

Syntax Description

all	Displays a table of all configured connections.
elements	Displays registered hardware or software interworking elements.
name	Displays a connection that has been named by using the **connect** global configuration command. The name you enter is case sensitive and must match the configured name exactly.
id	Displays the status of a connection that you specify by an identification number or range of identification numbers. The router assigns these IDs automatically in the order in which they were created, beginning with 1. The **show connect all** command displays these IDs.
port	Displays the status of a connection that you specify by indicating the type of controller (T1 or E1) and location of the interface.
T1	Specifies a T1 controller.
E1	Specifies an E1 controller.
slot/*port*	The location of the T1 or E1 controller port whose connection status you want to see. Valid values for *slot* and *port* are 0 and 1. The slash must be entered.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

This command shows drop-and-insert connections on the Cisco 2600 and 3600 series.

The command displays different information in different formats, depending on the keyword that you use.

Examples

The following examples show how the same tabular information appears when you enter different keywords:

```
Router# show connect all

ID   Name               Segment 1            Segment 2           State
========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP

Router# show connect id 1-2

ID   Name               Segment 1            Segment 2           State
========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP

Router# show connect port t1 1/1

ID   Name               Segment 1            Segment 2           State
========================================================================
1    Test              -T1 1/0 01           -T1 1/1 02           ADMIN UP
2    Test2             -T1 1/0 03           -T1 1/1 04           ADMIN UP
```

The following examples show details about specific connections, including the number of time slots in use and the switching elements:

```
Router# show connect id 2

Connection: 2 - Test2
 Current State: ADMIN UP
 Segment 1: -T1 1/0 03
  TDM timeslots in use: 14-18 (5 total)
 Segment 2: -T1 1/1 04
  TDM timeslots in use: 14-18
Internal Switching Elements: VIC TDM Switch

Router# show connect name Test

 Connection: 1 - Test
 Current State: ADMIN UP
 Segment 1: -T1 1/0 01
  TDM timeslots in use: 1-13 (13 total)
 Segment 2: -T1 1/1 02
  TDM timeslots in use: 1-13
Internal Switching Elements: VIC TDM Switch
```

Related Commands

Command	Description
connect	Defines connections between T1 or E1 controller ports for Drop and Insert.
tdm-group	Configures a list of time slots for creating clear channel groups (pass-through) for TDM cross-connect.

show controllers rs366

To display information about the RS-366 video interface on the video dialing module (VDM), use the **show controllers rs366** command in privileged EXEC mode.

show controllers rs366 *slot port*

Syntax Description

slot	Slot location of the VDM module. On the Cisco MC3810 multiservice concentrator, this value is either 1 or 2. If you do not enter the correct location, the command is rejected.
port	Port location of the EIA/TIA-366 interface in the VDM module. On the Cisco MC3810 multiservice concentrator, this value is 0.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Examples

On a Cisco MC3810 multiservice concentrator, the following example displays information about the RS-366 controller:

```
Router# show controller rs366 0 1

RS366:driver is initialized in slot 1, port 0:

STATUS STATE LSR  LCR  ICSR EXT  T1     T2     T3     T4     T5
0x02   0x01  0x00 0x50 0xE0 0x00 5000   5000   5000   20000  10000
Dial string:
121C
```

Table 33 describes the significant fields shown in the display.

Table 33 show controllers Field Descriptions

Field	Description
STATUS	Last interrupt status.
STATE	Current state of the state machine.
LSR	Line status register of the VDM.
LCR	Line control register of the VDM.

Table 33 show controllers Field Descriptions (continued)

Field	Description
ICSR	Interrupt control and status register of the VDM.
EXT	Extended register of the VDM.
T1 through T5	Timeouts 1 through 5 of the watchdog timer, in milliseconds.
Dial string	Most recently dialed number collected by the driver. 0xC at the end of the string indicates the EON (end of number) character.

show controllers timeslots

To show the channel-associated signaling (CAS) and ISDN PRI state in detail, use the **show controllers timeslots** command in privileged EXEC mode.

show controllers t1/e1 *controller-number* **timeslots** *timeslot-range*

Syntax Description

tl/e1	Specifies the type of interface.
controller-number	Specifies the controller number of CAS or ISDN PRI time slot. Range 0 through 7.
timeslots	Displays DS0 information.
timeslot-range	Specifies time slot range 1 through 31 for E1, 1 through 24 for T1.

Defaults

No default

Command Modes

Privileged EXEC

Command History

Release	Modification
10.0	This command was introduced.
12.1(3)T	The **timeslots** keyword was added.
12.1(5)T	Support for Cisco AS5400 universal access servers was added.

Usage Guidelines

Use the **show controllers t1/e1 timeslots** command to display the CAS and ISDN PRI channel state in detail. This command shows whether the DS0 channels of a controller are in idle, in-service, maintenance, or busyout states. Enter the **show controllers t1/e1** command to display statistics about the T1 or E1 links.

Examples

The following example shows that the CAS state is enabled on the Cisco AS5300 universal access server with a T1 PRI card:

```
Router# show controllers timeslots
T1 1 is up:
Loopback: NONE
DS0  Type       Modem    <->     Service       Channel       Rx          Tx
                                 State         State        A B C D     A B C D
------------------------------------------------------------------------------------------
   1    cas-modem   1       in     insvc       connected     1  1  1  1     1  1  1  1
   2    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   3    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   4    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   5    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   6    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   7    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   8    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
   9    cas          -       -     insvc       idle          0  0  0  0     0  0  0  0
```

```
  10   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  11   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  12   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  13   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  14   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  15   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  16   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  17   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  18   cas          -       -      maint      static-bo     0  0  0  0     1  1  1  1
  19   cas          -       -      maint      dynamic-bo    0  0  0  0     1  1  1  1
  20   cas          -       -      maint      dynamic-bo    0  0  0  0     1  1  1  1
  21   cas          -       -      maint      dynamic-bo    0  0  0  0     1  1  1  1
  22   unused
  23   unused
  24   unused
```

The following example shows that the ISDN PRI state is enabled on the Cisco AS5300 universal access server with a T1 PRI card:

```
T1 2 is up:
Loopback: NONE
DS0 Type         Modem    <->  Service   Channel     Rx        Tx
                               State     State       A B C D   A B C D
---------------------------------------------------------------------------
 1  pri          -        -    insvc     idle
 2  pri          -        -    insvc     idle
 3  pri          -        -    insvc     idle
 4  pri          -        -    insvc     idle
 5  pri          -        -    insvc     idle
 6  pri          -        -    insvc     idle
 7  pri          -        -    insvc     idle
 8  pri          -        -    insvc     idle
 9  pri          -        -    insvc     idle
10  pri          -        -    insvc     idle
11  pri          -        -    insvc     idle
12  pri          -        -    insvc     idle
13  pri          -        -    insvc     idle
14  pri          -        -    insvc     idle
15  pri          -        -    insvc     idle
16  pri          -        -    insvc     idle
17  pri          -        -    insvc     idle
18  pri          -        -    insvc     idle
19  pri          -        -    insvc     idle
20  pri          -        -    insvc     idle
21  pri-modem    2        in   insvc     busy
22  pri-modem    1        out  insvc     busy
23  pri-digi     -        in   insvc     busy
24  pri-sig      -        -    outofsvc  reserved
```

show controllers voice

To display information about voice-related hardware, use the **show controllers voice** command in privileged EXEC mode.

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XQ	This command was introduced on the Cisco 1750.

Usage Guidelines

This command displays interface status information that is specific to voice-related hardware, such as the registers of the TDM switch, the host port interface of the digital signal processor (DSP), and the DSP firmware versions. The information displayed is generally useful only for diagnostic tasks performed by technical support.

Examples

The following is an example of the output from the **show controllers voice** command:

```
Router# show controllers voice

EPIC Switch registers:
STDA 0xFF STDB 0xFF SARA 0xAD SARB 0xFF SAXA 0xFF SAXB 0x0 STCR 0x3F
MFAIR 0x3F
STAR 0x65 OMDR 0xE2 VNSR 0x0 PMOD 0x4C PBNR 0xFF POFD 0xF0 POFU 0x18
PCSR 0x1 PICM 0x0 CMD1 0xA0 CMD2 0x70 CBNR 0xFF CTAR 0x2 CBSR 0x20 CSCR
0x0

DSP 0 Host Port Interface:
HPI Control Register 0x202
InterfaceStatus 0x2A MaxMessageSize 0x80
RxRingBufferSize 0x6 TxRingBufferSize 0x9
pInsertRx 0x4 pRemoveRx 0x4 pInsertTx 0x6 pRemoveTx 0x6

Rx Message 0:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 0000 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0

Rx Message 1:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 0000 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
```

```
0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB

Rx Message 2:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 0000 54DA 61F5 EF60 DA53
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0

Rx Message 3:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 0000 C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1

Rx Message 4:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 0000 DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C

Rx Message 5:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 0000 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835

Tx Message 0:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC6 5F08 9181 0000 003C DD5B DC5E E161 E468
0020:   FAFD 6CE1 5AD3 53D1 53D7 61EC EA59 CF4A C644 C344
0040:   CA4E D86C 60D0 48C2 3EBD 3CBD 3EC0 47CF 5976 DF4F
0060:   C945 C242 C146 C94E D668 73DB 54CE 4DCC 4DCE 53DB
0080:   64F9 ED63 DC59 DA58 DC5D E46C

Tx Message 1:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDC 3E48 3B24 0000 003C 5B5B 5D62 6A76 FCF5
0020:   F5F9 7D78 7374 7CF5 EAE1 DDDA DBDD E7FE 6559 514E
0040:   4D4F 5663 EFD8 CDC8 C6C6 CAD1 E760 4E46 403F 4047
0060:   5173 D5C7 BFBC BCBE C5D4 6D4C 3F3B 3939 3D46 5ADB
0080:   C5BC B7B6 B8BD C8E8 4F3F 3835

Tx Message 2:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC7 5F08 91D1 0000 003C 7DF1 69E5 63E1 63E2
0020:   6E7C ED67 DE5D DB5C DC60 EC7E 6BE1 58D3 50CD 4DCE
0040:   50D2 5AE5 7868 DA52 CE4A C746 C647 C94B D25A EAF4
0060:   5DD7 4FCD 4ACA 4ACC 4FD3 5DE8 F769 DC58 D352 D253
0080:   D65B E573 6CDF 59D3 4ECF 4FD0

Tx Message 3:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDD 3E48 3B74 0000 003C 3437 3D4C F0C8 BBB5
0020:   B2B3 B7BF D25B 4138 3331 3339 435F CFBD B6B2 B1B4
```

```
0040:   BBC8 7E48 3B34 3131 363D 4FDE C3B9 B3B1 B3B8 C2DB
0060:   533F 3833 3235 3B48 71CC BDB7 B4B5 B8BF CF67 483D
0080:   3836 383C 455B DAC6 BDB9 B9BB

Tx Message 4:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC8 5F08 9221 0000 003C 54DA 61F5 EF60 DA53
0020:   CF4F CD4E D256 DB63 FCEE 5FDA 55D1 50CF 4FD3 56D8
0040:   5DE1 6E7C EC60 DC59 D655 D456 D85D DF6A F4F4 69E2
0060:   5CDD 5BDC 5BDE 61E9 6DF1 FF76 F16D E96A E566 EA6A
0080:   EB6F F16D EF79 F776 F5F5 73F0

Tx Message 5:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDE 3E48 3BC4 0000 003C C0CC EC54 453E 3C3C
0020:   3F47 56F3 D1C7 C1BF C0C6 CEE1 6752 4A46 4648 4E59
0040:   6FE4 D6CF CDCE D2DA E57E 675E 5B5B 5E62 6B76 FCF6
0060:   F6FA 7D75 7373 7BF5 EAE1 DCDA DADD E6FE 6559 514D
0080:   4D4E 5563 EFD9 CDC8 C5C6 CAD1

Tx Message 6:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDA 3E48 3A84 0000 003C E75F 4E46 403F 4147
0020:   5174 D5C7 BFBC BCBE C5D4 6C4C 3F3B 3939 3D46 5BDA
0040:   C5BC B7B6 B8BD C8E9 4F3F 3834 3437 3D4C EEC8 BBB5
0060:   B2B3 B8BF D35A 4138 3331 3339 435F CEBD B6B1 B1B4
0080:   BBC9 7C48 3B34 3131 363D 4FDE

Tx Message 7:
packet_length 100 channel_id 1 packet_id 0 process id 0x1
0000:   0000 4AC5 5F08 9131 0000 003C 66DE 66EB 67EE FE6E
0020:   F7E7 6B68 E068 EE6A DF5C DF62 EDF1 6FF2 7A78 67DC
0040:   5EDF 62E7 64E6 66E0 7071 EA69 F86E E260 DE5D E665
0060:   EB75 F0FB 6DE9 64E4 69E3 66EA 67E9 6DF9 F177 EC6E
0080:   EB6E F876 F875 7D6E E966 E05D

Tx Message 8:
packet_length 100 channel_id 2 packet_id 0 process id 0x1
0000:   0000 1CDB 3E48 3AD4 0000 003C C2B9 B3B1 B3B8 C2DC
0020:   523F 3733 3235 3C49 72CB BDB7 B4B5 B8BF CF67 483C
0040:   3836 373C 455C DAC6 BDB9 B9BB C0CC EE54 453E 3C3C
0060:   3F47 56F1 D1C7 C1BF C0C6 CEE1 6651 4A46 4648 4D59
0080:   70E3 D6CF CDCE D2D9 E67E 675E

Bootloader 1.8, Appn 3.1
Application firmware 3.1.8, Built by claux on Thu Jun 17 11:00:05 1999

VIC Interface Foreign Exchange Station 0/0, DSP instance (0x19543C0)
Singalling channel num 128 Signalling proxy 0x0 Signaling dsp 0x19543C0
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 1
received 0 packets, 0 bytes, 0 gaint packets
0 drops, 0 no buffers, 0 input errors 0 input overruns
650070 bytes output, 4976 frames output, 0 output errors, 0 output
underrun
0 unaligned frames

VIC Interface Foreign Exchange Station 0/1, DSP instance (0x1954604)
Singalling channel num 129 Signalling proxy 0x0 Signaling dsp 0x1954604
tx outstanding 0, max tx outstanding 32
ptr 0x0, length 0x0, max length 0x0
dsp_number 0, Channel ID 2
received 0 packets, 0 bytes, 0 gaint packets
```

```
0 drops, 0 no buffers, 0 input errors 0 input overruns
393976 bytes output, 3982 frames output, 0 output errors, 0 output
underrun
0 unaligned frames
```

Related Commands

Command	Description
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show interface dspfarm	Displays hardware informatio,n including DRAM, SRAM, and the revision-level information on the line card.
show voice dsp	Displays the current status of all DSP voice channels on the Cisco MC3810 multiservice concentrator.
show voice port	Displays configuration information about a specific voice port.

show csm

To display the call switching module (CSM) statistics for a particular digital signal processor (DSP) channel or all DSP channels or for a specific modem or DSP channel, use the **show csm** command in privileged EXEC mode.

Cisco AS5300 Universal Access Server

show csm {**modem** [*slot*/*port* | *modem-group-number*] | **voice** [*slot*/*dspm*/*dsp*/*dsp-channel*]}

Cisco AS5800 Universal Access Server

show csm voice [*shelf/slot/port*]

Syntax Description

modem	Specifies CSM call statistics for modems.
voice	Specifies CSM call statistics for DSP channels.
slot/*port*	(Optional) Specifies the location (and thereby the identity) of a specific modem.
modem-group-number	(Optional) Displays configuration for the dial peer identified by the argument *modem-group-number.* Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
slot/dspm/*dsp*/*dsp-channel*	(Optional) Identifies the location of a particular DSP channel.
shelf/slot/port	(Optional) Identifies the location of the voice interface card.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced.
12.0(3)T	Port-specific values for the Cisco AS5300 universal access server were added.
12.0(7)T	Port-specific values for the Cisco AS5800 were added.

Usage Guidelines

This command shows the information related to CSM, which includes the DSP channel, the start time of the call, the end time of the call, and the channel on the controller used by the call.

Use the **show csm modem** command to display the CSM call statistic information for a specific modem, for a group of modems, or for all modems. If a *slot/port* argument is specified, then CSM call statistics are displayed for the specified modem. If the *modem-group-number* argument is specified, the CSM call statistics for all of the modems associated with that modem group are displayed. If no keyword is specified, CSM call statistics for all modems on the Cisco AS5300 universal access server are displayed.

Use the **show csm voice** command to display CSM statistics for a particular DSP channel. If the *slot/dspm/dsp/dsp-channel* or *shelf/slot/port* argument is specified, the CSM call statistics for calls using the identified DSP channel will be displayed. If no argument is specified, all CSM call statistics for all DSP channels will be displayed.

Examples

The following is sample output from the Cisco AS5300 universal access server for the **show csm voice** command:

```
Router# show csm voice 2/4/4/0

 slot 2, dspm 4, dsp 4, dsp channel 0,
 slot 2, port 56, tone, device_status(0x0002): VDEV_STATUS_ACTIVE_CALL.

csm_state(0x0406)=CSM_OC6_CONNECTED, csm_event_proc=0x600E2678, current call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
wdt_timestamp_started is not activated
wait_for_dialing:False, wait_for_bchan:False
pri_chnl=TDM_PRI_STREAM(s0, u0, c22), tdm_chnl=TDM_DSP_STREAM(s2, c27)
dchan_idb_start_index=0, dchan_idb_index=0, call_id=0xA003, bchan_num=22
csm_event=CSM_EVENT_ISDN_CONNECTED, cause=0x0000
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=3
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, stat_busyout=0
oobp_failure=0
call_duration_started=00:06:53, call_duration_ended=00:00:00, total_call_duration=00:00:44
The calling party phone number = 408
The called party phone number  = 5271086
total_free_rbs_timeslot = 0, total_busy_rbs_timeslot = 0, total_dynamic_busy_rbs_timeslot
= 0, total_static_busy_rbs_timeslot = 0,
total_sw56_rbs_timeslot = 0, total_sw56_rbs_static_bo_ts = 0,
total_free_isdn_channels = 21, total_busy_isdn_channels = 0,total_auto_busy_isdn_channels
= 0,
min_free_device_threshold = 0
```

The following is sample output from the Cisco AS5800 for the **show csm voice** command:

```
Router# show csm voice 1/8/19

 shelf 1, slot 8, port 19
VDEV_INFO:slot 8, port 19
vdev_status(0x00000401):VDEV_STATUS_ACTIVE_CALL.VDEV_STATUS_HASLOCK.
csm_state(0x00000406)=CSM_OC6_CONNECTED, csm_event_proc=0x60868B8C, current
call thru PRI line
invalid_event_count=0, wdt_timeout_count=0
watchdog timer is not activated
wait_for_bchan:False
pri_chnl=(T1 1/0/0:22), vdev_chnl=(s8, c19)
start_chan_p=0, chan_p=62436D58, call_id=0x800D, bchan_num=22
The calling party phone number =
The called party phone number  = 7511
ring_no_answer=0, ic_failure=0, ic_complete=0
dial_failure=0, oc_failure=0, oc_complete=1
oc_busy=0, oc_no_dial_tone=0, oc_dial_timeout=0
remote_link_disc=0, busyout=0, modem_reset=0
call_duration_started=3d16h, call_duration_ended=00:00:00,
total_call_duration=00:00:00
```

Table 34 describes the significant fields shown in the display.

Table 34 show csm voice Field Descriptions

Field	Description
slot	Slot where the VFC resides.
shelf/slot/port	Specifies the T1 or E1 controller.
dspm/dsp/dsp channel	Indicates which DSP channel is engaged in this call.
dsp	Indicates the DSP through which this call is established.
slot/port	Logical port number for the device. This is equivalent to the DSP channel number. The port number is derived as follows: • (max_number_of_dsp_channels per dspm=12) * the dspm # (0-based) + • (max_number_of_dsp_channels per dsp=2) * the dsp # (0-based) + the dsp channel number (0-based).
tone	Indicates which signaling tone is being used (DTMF, MF, R2). This only applies to CAS calls. Possible values are as follows: • mf • dtmf • r2-compelled • r2-semi-compelled • r2-non-compelled

Table 34 show csm voice Field Descriptions (continued)

Field	Description
device_status	The status of the device. Possible values are as follows: • VDEV_STATUS_UNLOCKED—Device is unlocked (meaning that it is available for new calls). • VDEV_STATUS_ACTIVE_WDT—Device is allocated for a call and the watchdog timer is set to time the connection response from the central office. • VDEV_STATUS_ACTIVE_CALL—Device is engaged in an active, connected call. • VDEV_STATUS_BUSYOUT_REQ—Device is requested to busyout; does not apply to voice devices. • VDEV_STATUS_BAD—Device is marked as bad and not usable for processing calls. • VDEV_STATUS_BACK2BACK_TEST—Modem is performing back-to-back testing (for modem calls only). • VDEV_STATUS_RESET—Modem needs to be reset (for modem only). • VDEV_STATUS_DOWNLOAD_FILE—Modem is downloading a file (for modem only). • VDEV_STATUS_DOWNLOAD_FAIL—Modem has failed during downloading a file (for modem only). • VDEV_STATUS_SHUTDOWN—Modem is not powered up (for modem only). • VDEV_STATUS_BUSY—Modem is busy (for modem only). • VDEV_STATUS_DOWNLOAD_REQ—Modem is requesting connection (for modem only).

Table 34 show csm voice Field Descriptions (continued)

Field	Description
csm_state	CSM call state of the current call (PRI line) associated with this device. Possible values are as follows: • CSM_IDLE_STATE—Device is idle. • CSM_IC_STATE—A device has been assigned to an incoming call. • CSM_IC1_COLLECT_ADDR_INFO—A device has been selected to perform ANI/DNIS address collection for this call. ANI/DNIS address information collection is in progress. The ANI/DNIS is used to decide whether the call should be processed by a modem or a voice DSP. • CSM_IC2_RINGING—The device assigned to this incoming call has been told to get ready for the call. • CSM_IC3_WAIT_FOR_SWITCH_OVER—A new device is selected to take over this incoming call from the device collecting the ANI/DNIS address information. • CSM_IC4_WAIT_FOR_CARRIER—This call is waiting for the CONNECT message from the carrier. • CSM_IC5_CONNECTED—This incoming call is connected to the central office. • CSM_IC6_DISCONNECTING—This incoming call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process. • CSM_OC_STATE —An outgoing call is initiated. • CSM_OC1_REQUEST_DIGIT—The device is requesting the first digit for the dial-out number. • CSM_OC2_COLLECT_1ST_DIGIT—The first digit for the dial-out number has been collected. • CSM_OC3_COLLECT_ALL_DIGIT—All the digits for the dial-out number have been collected. • CSM_OC4_DIALING—This call is waiting for a dsx0 (B channel) to be available for dialing out. • CSM_OC5_WAIT_FOR_CARRIER—This (outgoing) call is waiting for the central office to connect. • CSM_OC6_CONNECTED—This (outgoing) call is connected. • CSM_OC7_BUSY_ERROR—A busy tone has been sent to the device (for VoIP call, no busy tone is sent; just a DISCONNECT INDICATION message is sent to the VTSP module),and this call is waiting for a DISCONNECT message from the VTSP module (or ONHOOK message from the modem) to complete the disconnect process. • CSM_OC8_DISCONNECTING—The central office has disconnected this (outgoing) call, and the call is waiting for a DISCONNECT message from the VTSP module to complete the disconnect process.

Table 34 show csm voice Field Descriptions (continued)

Field	Description
csm_state: invalid_event_count=	Number of invalid events received by the CSM state machine.
wdt_timeout_count=	Number of times the watchdog timer is activated for this call.
wdt_timestamp_started	Indicates whether the watchdog timer is activated for this call.
wait_for_dialing:	Indicates whether this (outgoing) call is waiting for a free digit collector to become available to dial out the outgoing digits.
wait_for_bchan:	Indicates whether this (outgoing) call is waiting for a B channel to send the call out on.
pri_chnl=	Indicates which type of TDM stream is used for the PRI connection. For PRI and CAS calls, it will always be TDM_PRI_STREAM.
tdm_chnl=	Indicates which type of TDM stream is used for the connection to the device used to process this call. In the case of a VoIP call, this will always be set to TDM_DSP_STREAM.
dchan_idb_start_index=	First index to use when searching for the next IDB of a free D channel.
dchan_idb_index=	Index of the currently available IDB of a free D channel.
csm_event=	Event just passed to the CSM state machine.
cause	Event cause.
ring_no_answer=	Number of times a call failed because there was no response.
ic_failure=	Number of failed incoming calls.
ic_complete=	Number of successful incoming calls.
dial_failure=	Number of times a connection failed because there was no dial tone.
oc_failure=	Number of failed outgoing calls.
oc_complete=	Number of successful outgoing calls.
oc_busy=	Number of outgoing calls whose connection failed because there was a busy signal.
oc_no_dial_tone=	Number of outgoing calls whose connection failed because there was no dial tone.
oc_dial_timeout=	Number of outgoing calls whose connection failed because the timeout value was exceeded.
call_duration_started=	Indicates the start of this call.
call_duration_ended=	Indicates the end of this call.
total_call_duration=	Indicates the duration of this call.
The calling party phone number =	Calling party number as given to CSM by ISDN.
The called party phone number =	Called party number as given to CSM by ISDN.
total_free_rbs_time slot =	Total number of free RBS (CAS) time slots available for the whole system.

Table 34 show csm voice Field Descriptions (continued)

Field	Description
total_busy_rbs_time slot =	Total number of RBS (CAS) time slots that have been busied-out. This includes both dynamically and statically busied out RBS time slots.
total_dynamic_busy_rbs_time slot =	Total number of RBS (CAS) time slots that have been dynamically busied out.
total_static_busy_rbs_time slot =	Total number of RBS (CAS) time slots that have been statically busied out (that is, they are busied out using the CLI command).
total_free_isdn_channels =	Total number of free ISDN channels.
total_busy_isdn_channels =	Total number of busy ISDN channels.
total_auto_busy_isdn_channels =	Total number of ISDN channels that are automatically busied out.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show num-exp	Displays how number expansions are configured.
show voice port	Displays configuration information about a specific voice port.

show dial-peer video

To display dial-peer configuration, use the **show dial-peer video** command in privileged EXEC mode.

show dial-peer video [*number*] [**summary**]

Syntax Description

number	(Optional) A specific video dial peer. This option displays configuration information for a single dial peer identified by the argument *number*. Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
summary	(Optional) Displays a summary of all video dial peer information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to review video dial peer configuration.

Examples

On a Cisco MC3810 multiservice concentrator, the following example displays detailed information about all configured video dial peers:

```
Router# show dial-peer video

Video Dial-Peer 1
      type = videocodec, destination-pattern = 111
      port signal = 1/0, port media = Serial1
      nsap = 47.0091810000000050E201B101.00107B09C6F2.C8
Video Dial-Peer 2
      type = videoatm,   destination-pattern = 222
      session-target = ATM0 svc nsap 47.0091810000000050E201B101.00E01E92ADC2.C8
Video Dial-Peer 3
      type = videoatm,   destination-pattern = 333
      session-target = ATM0 pvc 70/70
```

show dial-peer voice

To display configuration information for dial peers, use the **show dial-peer voice** command in privileged EXEC mode.

show dial-peer voice [*number*] [**summary**]

Syntax Description

number	(Optional) A specific dial peer. This option displays configuration information for a single dial peer identified by the *number* argument. Valid entries are any integers that identify a specific dial peer, from 1 to 32767.
summary	(Optional) Displays a summary of all voice dial peers.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced.
11.3(1)MA	The **summary** keyword was added for the Cisco MC3810 multiservice concentrator.
12.0(3)XG	This command was modified to support Voice over Frame Relay (VoFR) for the Cisco 2600 series and Cisco 3600 series routers.
12.0(4)T	Support was added for VoFR for the Cisco 7200 series routers.
12.1(3)T	This command was modified for Modem Passthrough over Voice over IP on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **show dial-peer voice** privileged EXEC command to display the configuration for all Voice over IP (VoIP) and plain old telephone service (POTS) dial peers configured for the router. To show configuration information for only one specific dial peer, use the argument *number* to identify the dial peer.

Examples

The following is sample output from the **show dial-peer voice** command for a POTS dial peer:

```
Router# show dial-peer voice 1

VoiceEncapPeer1
        tag = 1, dest-pat = `+14085291000',
        answer-address = `',
        group = 0, Admin state is up, Operation state is down
        Permission is Both,
        type = pots, prefix = `',
        session-target = `', voice port =
        Connect Time = 0, Charged Units = 0
```

```
        Successful Calls = 0, Failed Calls = 0
        Accepted Calls = 0, Refused Calls = 0
        Last Disconnect Cause is ""
        Last Disconnect Text is ""
        Last Setup Time = 0
```

The following is sample output from the **show dial-peer voice** command for a VoIP dial peer:

```
Router# show dial-peer voice 10

VoiceOverIpPeer10
        tag = 10, dest-pat = `',
        incall-number = `+14087',
        group = 0, Admin state is up, Operation state is down
        Permission is Answer,
        type = voip, session-target = `',
        sess-proto = cisco, req-qos = bestEffort,
        acc-qos = bestEffort,
        fax-rate = voice, codec = g729r8,
        Expect factor = 10,Icpif = 30, VAD = disabled, Poor QOV Trap = disabled,
        Connect Time = 0, Charged Units = 0
        Successful Calls = 0, Failed Calls = 0
        Accepted Calls = 0, Refused Calls = 0
        Last Disconnect Cause is ""
        Last Disconnect Text is ""
        Last Setup Time = 0
```

Table 35 provides an alphabetical listing of the **show dial-peer voice** output fields and a description of each field.

Table 35 show dial-peer voice Field Descriptions

Field	Description
Accepted Calls	Number of calls accepted from this peer since system startup.
acc-qos	Lowest acceptable quality of service configured for calls for this peer.
Admin state	Administrative state of this peer.
answer-address	Answer address configured for this dial peer.
Charged Units	Total number of charging units applying to this peer since system startup. The unit of measure for this field in hundredths of a second.
codec	Default voice coder rate of speech for this peer.
Connect Time	Accumulated connect time to the peer since system startup for both incoming and outgoing calls. The unit of measure for this field is in hundredths of a second.
dest-pat	Destination pattern (telephone number) for this peer.
DTMF Relay	Indicates whether or not dual-tone multifrequency (DTMF) relay has been enabled, by using the **dtmf-relay** command, for this dial peer.
Expect factor	User-requested Expectation Factor of voice quality for calls through this peer.
fax-rate	Fax transmission rate configured for this peer.
Failed Calls	Number of failed call attempts to this peer since system startup.
group	Group number associated with this peer.

Table 35 show dial-peer voice Field Descriptions (continued)

Field	Description
huntstop	Indicates whether dial-peer hunting has been turned on, by using the **huntstop** command, for this dial peer.
Icpif	Configured Calculated Planning Impairment Factor (ICPIF) value for calls sent by a dial peer.
incall-number	Full E.164 telephone number to be used to identify the dial peer.
incoming called-number	Indicates the incoming called number if it has been set by using the **incoming-called number** command.
information type	Information type for this call; for example, voice or fax.
Last Disconnect Cause	Encoded network cause associated with the last call. This value will be updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Modem passthrough	Modem pass-through signaling method is named signaling event (NSE).
Operation state	Operational state of this peer.
Payload type	NSE payload type.
Permission	Configured permission level for this peer.
Poor QOV Trap	Whether Poor Quality of Voice trap messages have been enabled or disabled.
Redundancy	Packet redundancy (RFC 2198) for modem traffic.
Refused Calls	Number of calls from this peer refused since system startup.
req-qos	Configured requested quality of service for calls for this dial peer.
session-target	Session target of this peer.
sess-proto	Session protocol to be used for Internet calls between local and remote routers through the IP backbone.
Successful Calls	Number of completed calls to this peer.
tag	Unique dial peer ID number.
VAD	Whether voice activation detection (VAD) is enabled for this dial peer.

Related Commands

Command	Description
show call active voice	Displays the Voice over IP active call table.
show call history voice	Displays the Voice over IP call history table.
show num-exp	Displays how the number expansions are configured in Voice over IP.
show voice port	Displays configuration information about a specific voice port.

show dialplan incall number

To show which plain old telephone service (POTS) dial peer is matched for a specific calling number or voice port, use the **show dialplan incall number** command in privileged EXEC mode.

show dialplan incall *voice-port* **number** *calling-number* [**timeout**]

Syntax Description

voice-port	Specifies the voice port location. The syntax of this argument is platform-specific. For information on the syntax for a particular platform, see the **voice-port** global configuration command.
calling-number	Specifies the calling number or ANI of the incoming voice call.
timeout	(Optional) Allows matching for variable-length destination patterns.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.2(8)T	The **timeout** keyword was added.

Usage Guidelines

Use the **show dialplan incall number** command as a troubleshooting tool to determine which POTS dial peer is matched for an incoming call, for the selected calling number and voice port. When using the **show dialplan incall number** command, the router attempts to match these items in the order listed:

1. Calling number with answer-address configured in dial peer
2. Calling number with destination-pattern configured in dial peer
3. Voice port with voice port configured in dial peer

The router first attempts to match a dial peer based on the calling number (ANI). If the router is unable to match a dial peer based on the calling number, it matches the call to a POTS dial peer based on the selected voice interface. If more than one dial peer uses the same voice port, the router selects the first matching dial peer. Use the **timeout** keyword to enable matching variable-length destination patters associated with dial peers. This can increase you r chances of finding a match for the dial peer number you specify.

Note For actual voice calls coming into the router, the router attempts to match the called number (the dialed number identification service [DNIS] number) with the incoming called-number configured in a dial peer. The router, however, does not consider the called number when using the **show dialplan incall number** command.

Examples

The following example shows that an incoming call from interface 1/0/0:D with a calling number of 12345 is matched to POTS dial peer 10:

```
Router# show dialplan incall 1/0/0:D number 12345

Macro Exp.: 12345

VoiceEncapPeer10
        information type = voice,
        tag = 10, destination-pattern = `123..',
        answer-address = `', preference=0,
        numbering Type = `unknown'
        group = 10, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `',
        forward-digits default
        session-target = `', voice-port = `1/0/0:D',
        direct-inward-dial = disabled,
        digit_strip = enabled,

        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,

        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 12345   Digits: 3
Target:
```

The following example shows that if no dial peer has a destination pattern or answer address that matches the calling number of 888, the incoming call is matched to POTS dial peer 99, because the call comes in on voice port 1/0/1:D, which is the voice port configured for this dial peer:

```
Router# show dialplan incall 1/0/1:D number 888

Macro Exp.: 888

VoiceEncapPeer99
        information type = voice,
        tag = 99, destination-pattern = `99...',
        answer-address = `', preference=1,
        numbering Type = `national'
        group = 99, Admin state is up, Operation state is up,
        incoming called-number = `', connections/maximum = 0/unlimited,
        DTMF Relay = disabled,
        huntstop = disabled,
        in bound application associated: DEFAULT
        out bound application associated:
        permission :both
        incoming COR list:maximum capability
        outgoing COR list:minimum requirement
        type = pots, prefix = `5',
```

```
        forward-digits 4
        session-target = `', voice-port = `1/0/1:D',
        direct-inward-dial = enabled,
        digit_strip = enabled,

        register E.164 number with GK = TRUE
        Connect Time = 0, Charged Units = 0,
        Successful Calls = 0, Failed Calls = 0,
        Accepted Calls = 0, Refused Calls = 0,
        Last Disconnect Cause is "",
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched:    Digits: 0
Target:
```

Table 36 describes the significant fields shown in the display.

Table 36 show dialplan number Field Descriptions

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the calling number entered.
tag	Unique number identifying the dial peer.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address (calling number) configured for this dial peer.
preference	Hunt group preference order set for this dial peer.
Admin state	Describes the administrative state of this dial peer.
Operation state	Describes the operational state of this dial peer.
incoming called-number	Called number (DNIS) configured for this dial peer.
DTMF Relay	Whether the **dtmf-relay** command is enabled or disabled for this dial peer.
huntstop	Whether the **huntstop** command is enabled or disabled for this dial peer.
in bound application associated	The IVR application that is associated with this dial peer when this dial peer is used for an inbound call leg.
out bound application associated	The IVR application that is associated with this dial peer when this dial peer is used for an outbound call leg.
type	Type of dial peer (POTS or VoIP).
prefix	The prefix number that is added to the front of the dial string before it is forwarded to the telephony device.
forward-digits	Which digits are forwarded to the telephony interface as configured using the **forward-digits** command.
session-target	Displays the configured session target (IP address or host name) for this dial peer.
voice-port	The voice port through which calls come into this dial peer.
direct-inward-dial	Whether the **direct-inward-dial** command is enabled or disabled for this dial peer.

Table 36 show dialplan number Field Descriptions (continued)

Field	Description
digit_strip	Whether digit stripping is enabled or disabled in the dial peer. Enabled is the default.
session-protocol	Session protocol to be used for Internet calls between local and remote router via the IP backbone.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this peer since system startup.
Accepted Calls	Number of calls from this peer accepted since system startup.
Refused Calls	Number of calls from this peer refused since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value will be updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
show dial peer voice	Displays the configuration information for dial peers.
show dialplan number	Displays which dial peer is matched for a particular telephone number.

show dialplan number

To show which dial peer is reached when a particular telephone number is dialed, use the **show dialplan number** command in privileged EXEC mode.

show dialplan number *dial string* [**huntstop**] [**timeout**]

Syntax Description

dial string	Specifies a particular destination pattern (telephone number).
huntstop	(Optional) Terminates further dial-peer hunting upon encountering the first dial string match.
timeout	(Optional) Allows matching for variable-length destination patterns.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.2(1)	The **huntstop** keyword was added.
12.2(8)T	The **timeout** keyword was added.

Usage Guidelines

The **show dialplan number** command is used to test whether the dial plan configuration is valid and working as expected. Use the **timeout** keyword to enable matching variable-length destination patters associated with dial peers. This can increase you r chances of finding a match for the dial peer number you specify.

Examples

The following example shows sample output from the **show dialplan number** command using the destination pattern of 1001:

```
Router# show dialplan number 1001

Macro Exp.: 1001

VoiceEncapPeer1003
         information type = voice,
         tag = 1003, destination-pattern = `1001',
         answer-address = `', preference=0,
         numbering Type = `unknown'
         group = 1003, Admin state is up, Operation state is up,
         incoming called-number = `', connections/maximum = 0/unlimited,
         DTMF Relay = disabled,
         huntstop = enabled,
         type = pots, prefix = `',
         forward-digits default
         session-target = `', voice-port = `1/1',
```

```
          direct-inward-dial = disabled,
          Connect Time = 0, Charged Units = 0,
          Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
          Accepted Calls = 0, Refused Calls = 0,
          Last Disconnect Cause is "",
          Last Disconnect Text is "",
          Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1004
          information type = voice,
          tag = 1004, destination-pattern = `1001',
          answer-address = `', preference=0,
          numbering Type = `unknown'
          group = 1004, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1002
          information type = voice,
          tag = 1002, destination-pattern = `1001',
          answer-address = `', preference=0,
          numbering Type = `unknown'
          group = 1002, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:

VoiceEncapPeer1001
          information type = voice,
          tag = 1001, destination-pattern = `1001',
          answer-address = `', preference=0,
          numbering Type = `unknown'
          group = 1001, Admin state is up, Operation state is up,
...
Matched: 1001   Digits: 4
Target:
```

The following example shows sample output from the **show dialplan number** command using the destination pattern of 1001 and the **huntstop** keyword:

```
Router# show dialplan number 1001 huntstop

 Macro Exp.: 1001

 VoiceEncapPeer1003
          information type = voice,
          tag = 1003, destination-pattern = `1001',
          answer-address = `', preference=0,
          numbering Type = `unknown'
          group = 1003, Admin state is up, Operation state is up,
          incoming called-number = `', connections/maximum = 0/unlimited,
          DTMF Relay = disabled,
          huntstop = enabled,
          type = pots, prefix = `',
          forward-digits default
          session-target = `', voice-port = `1/1',
          direct-inward-dial = disabled,
          Connect Time = 0, Charged Units = 0,
          Successful Calls = 0, Failed Calls = 0, Incomplete Calls = 0
          Accepted Calls = 0, Refused Calls = 0,
          Last Disconnect Cause is "",
```

```
        Last Disconnect Text is "",
        Last Setup Time = 0.
Matched: 1001   Digits: 4
Target:
```

Table 37 explains the significant fields shown in this example.

Table 37 show dialplan number Field Descriptions

Field	Description
Macro Exp.	Expected destination pattern for this dial peer.
VoiceEncapPeer	Dial peer associated with the destination pattern entered.
type	Type of dial peer (POTS or VoIP).
tag	Unique dial peer identifying number.
destination-pattern	Destination pattern (telephone number) configured for this dial peer.
answer-address	Answer address configured for this dial peer.
Admin state	Administrative state of this dial peer.
Operation state	Operational state of the dial peer.
session-target	Configured session target (IP address or host name) for this dial peer.
Connect Time	Unit of measure indicating the call connection time associated with this dial peer.
Charged Units	Number of call units charged to this dial peer.
Successful Calls	Number of completed calls to this peer since system startup.
Failed Calls	Number of uncompleted (failed) calls to this peer since system startup.
Accepted Calls	Number of calls accepted from this peer since system startup.
Refused Calls	Number of calls refused from this peer since system startup.
Last Disconnect Cause	Encoded network cause associated with the last call. This value will be updated whenever a call is started or cleared and depends on the interface type and session protocol being used on this interface.
Last Disconnect Text	ASCII text describing the reason for the last call termination.
Last Setup Time	Value of the System Up Time when the last call to this peer was started.
Matched	Destination pattern matched for this dial peer.
Target	Matched session target (IP address or host name) for this dial peer.

Related Commands

Command	Description
show dialplan incall number	Pairs different voice ports and telephone numbers together for troubleshooting Voice over IP.

show frame-relay vofr

To display information about the FRF.11 subchannels being used on Voice over Frame Relay (VoFR) data link connection identifiers (DLCIs), use the **show frame-relay vofr** command in privileged EXEC mode.

show frame-relay vofr [*interface* [*dlci* [*cid*]]]

Syntax Description

interface	(Optional) The specific interface type and number for which you wish to display FRF.11 subchannel information.
dlci	(Optional) The specific data link connection identifier for which you wish to display FRF.11 subchannel information.
cid	(Optional) The specific subchannel for which you wish to display information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco MC3810 multiservice concentrator.
12.0(4)T	This command was integrated in Cisco IOS Release 12.0(4)T.

Usage Guidelines

If this command is entered without a specified interface, FRF.11 subchannel information will be displayed for all VoFR interfaces and DLCIs configured on the router.

Note This command is currently not supported on the Cisco MC3810 multiservice concentrator for PVCs configured with the **vofr cisco** command or the **frame-relay interface-dlci voice-encap** command.

Examples

The following is sample output from the **show frame-relay vofr** command when an interface is not specified:

```
Router# show frame-relay vofr

interface         vofr-type   dlci   cid   cid-type
Serial0/0.1       VoFR        16     4     data
Serial0/0.1       VoFR        16     5     call-control
Serial0/0.1       VoFR        16     10    voice
Serial0/1.1       VoFR cisco  17     4     data
```

The following is sample output from the **show frame-relay vofr** command when an interface is specified:

```
Router# show frame-relay vofr serial0

interface          vofr-type    dlci    cid    cid-type
Serial0            VoFR         16      4      data
Serial0            VoFR         16      5      call-control
Serial0            VoFR         16      10     voice
```

The following is sample output from the **show frame-relay vofr** command when an interface and a DLCI are specified:

```
Router# show frame-relay vofr serial0 16

VoFR Configuration for interface Serial0

dlci vofr-type  cid cid-type          input-pkts    output-pkts    dropped-pkts
16   VoFR       4   data              0             0              0
16   VoFR       5   call-control      85982         86099          0
16   VoFR       10  voice             2172293       6370815        0
```

The following is sample output from the **show frame-relay vofr** command when an interface, a DLCI, and a CID are specified:

```
Router# show frame-relay vofr serial0 16 10

VoFR Configuration for interface Serial0 dlci 16

  vofr-type  VoFR      cid 10      cid-type voice
  input-pkts 2172293   output-pkts 6370815   dropped-pkts 0
```

Table 38 describes the significant fields shown in the display.

Table 38 show frame-relay vofr Field Descriptions

Field	Description
interface	Number of the interface that has been selected for observation of FRF.11 subchannels.
vofr-type	Type of VoFR DLCI being observed.
cid	The portion of the specified DLCI that is carrying the designated traffic type. A DLCI can be subdivided into 255 subchannels.
cid-type	Type of traffic carried on this subchannel.
input-pkts	Number of packets received by this subchannel.
output-pkts	Number of packets sent on this subchannel.
dropped-pkts	Total number of packets discarded by this subchannel.

Related Commands

Command	Description
show call active voice	Displays the contents of the active call table.
show call history voice	Displays the contents of the call history table.
show dial-peer voice	Displays configuration information and call statistics for dial peers.
show frame-relay fragment	Displays Frame Relay fragmentation details.

Command	Description
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show voice-port	Displays configuration information about a specific voice port.

show gatekeeper calls

To show the status of each ongoing call of which a gatekeeper is aware, use the **show gatekeeper calls** command in privileged EXEC mode.

show gatekeeper calls

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command introduced in Cisco IOS Release 11.3(2)NA was integrated into Cisco IOS Release 12.0(3)T.
12.0(5)T	The output for this command was changed.

Usage Guidelines

Use the **show gatekeeper calls** command to show all active calls currently being handled by a particular MCM gatekeeper. If you have forced a disconnect for either a particular call or all calls associated with a particular MCM gatekeeper by using the **clear h323 gatekeeper call** command, the system will not display information about those calls.

Examples

The following is sample output from the **show gatekeeper calls** command:

```
Router# show gatekeeper calls

Total number of active calls = 1.
                         GATEKEEPER CALL INFO
                         ====================
LocalCallID                        Age(secs)   BW
12-3339                            94          768(Kbps)
 Endpt(s):Alias        E.164Addr     CallSignalAddr  Port  RASSignalAddr   Port
   src EP:epA                        90.0.0.11       1720  90.0.0.11       1700
   dst EP:epB@zoneB.com
   src PX:pxA                        90.0.0.01       1720  90.0.0.01       24999
   dst PX:pxB                        172.21.139.90   1720  172.21.139.90   24999
```

Table 39 describes the significant fields shown in the display.

Table 39 show gatekeeper calls Field Descriptions

Field	Description
LocalCallID	Identification number of the call.
Age(secs)	The age of the call in seconds.
BW(Kbps)	The bandwidth in use, in kilobits per second.
Endpoint(s)	Lists the role of each endpoint (terminal, gateway, or proxy) in the call (originator, target, or proxy), and the call signaling and registration, admission, and status (RAS) protocol address.
Alias	H.323-ID or Email-ID of the endpoint.
E.164Addr	E.164 address of the endpoint.
CallSignalAddr	Call signaling IP address of the endpoint.
Port	Call signaling port number of the endpoint.
RASSignalAddr	RAS IP address of the endpoint.
Port	RAS port number of the endpoint.

Related Commands

Command	Description
clear h323 gateway call	Forces a specific call or all calls currently active on the gatekeeper to disconnect.

show gatekeeper endpoints

To display the status of all registered endpoints for a gatekeeper, use the **show gatekeeper endpoints** command in EXEC mode.

show gatekeeper endpoints

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.

Usage Guidelines

Use this command to display the status of all registered endpoints for a gatekeeper.

Examples

The following is sample output from the **show gatekeeper endpoints** command:

```
Router# show gatekeeper endpoints

CallsignalAddr   Port  RASSignalAddr   Port   Zone Name    Type     F
---------------  ----  -------------   -----  ----------   -----    --
172.21.127.8     1720  172.21.127.8    24999  sj-gk        MCU
           H323-ID:joe@cisco.com
172.21.13.88     1720  172.21.13.88    1719   sj-gk        VOIP-GW   O    H323-ID:la-gw
```

Table 40 describes the significant fields shown in the display.

Table 40 show gatekeeper endpoints Field Descriptions

Field	Description
CallsignalAddr	Call signaling IP address of the endpoint. If the endpoint is also registered with alias, a list of all aliases registered for that endpoint should be listed on the line below.
Port	Call signaling port number of the endpoint.
RASSignalAddr	Registration, admission, and status (RAS) protocol IP address of the endpoint.
Port	RAS port number of the endpoint.
Zone Name	Zone name (gatekeeper ID) that this endpoint registered in.

Table 40 show gatekeeper endpoints Field Descriptions (continued)

Field	Description
Type	The endpoint type (for example, terminal, gateway, or MCU).
F	S—Indicates that the endpoint is statically entered from the **alias** command rather than being dynamically registered through RAS messages. O—Indicates that the endpoint, which is a gateway, has sent notification that it is nearly out of resources.

Related Commands

Command	Description
show gatekeeper gw-type-prefix	Displays the gateway technology prefix table.
show gatekeeper zone status	Displays the status of zones related to a gatekeeper.
show gateway	Displays the current gateway status.

show gatekeeper gw-type-prefix

To display the gateway technology prefix table, use the **show gatekeeper gw-type-prefix** command in privileged EXEC mode.

show gatekeeper gw-type-prefix

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(5)T	The display format was modified for H.323 Version 2.

Usage Guidelines

Use the **show gatekeeper gw-type-prefix** command to display the gateway technology prefix table.

Examples

The following is sample output for a gatekeeper that is controlling two local zones, sj-gk and la-gk:

```
Router# show gatekeeper gw-type-prefix

GATEWAY TYPE PREFIX TABLE
===========================
Prefix:12#*     (Default gateway-technology)
  Zone sj-gk master gateway list:
    172.21.13.11:1720 sj-gw1
    172.21.13.22:1720 sj-gw2 (out-of-resources)
    172.21.13.33:1720 sj-gw3
  Zone sj-gk prefix 408....... priority gateway list(s):
   Priority 10:
    172.21.13.11:1720 sj-gw1
   Priority 5:
    172.21.13.22:1720 sj-gw2 (out-of-resources)
    172.21.13.33:1720 sj-gw3
Prefix:7#*     (Hopoff zone la-gk)
  Statically-configured gateways (not necessarily currently registered):
    1.1.1.1:1720
    2.2.2.2:1720
  Zone la-gk master gateway list:
    171.69.127.11:1720 la-gw1
    171.69.127.22:1720 la-gw2
```

Table 41 describes the fields contained in the **show gatekeeper gw-type-prefix** sample output.

Table 41 show gatekeeper gw-type-prefix Field Descriptions

Field	Description
Prefix	The technology prefix defined with the **gw-type-prefix** command.
Zone sj-gk master gateway list	A list of all the gateways registered to zone sj-gk with the technology prefix, under which they are listed. (This display shows that gateways sj-gw1, sj-gw2, and sj-gw3 have registered in zone sj-gk with the technology prefix 12#.)
Zone sj-gk prefix 408....... priority gateway list(s)	A list of prioritized gateways to handle calls to area code 408.
Priority 10	Highest priority level. Gateways listed following "Priority 10" are given the highest priority when selecting a gateway to service calls to the specified area code. (In this display, gateway sj-gw1 is given the highest priority to handle calls to the 408 area code.)
Priority 5	Any gateway that does not have a priority level assigned to it defaults to priority 5.
(out-of-resources)	Indication that the displayed gateway has sent a "low-in-resources" notification.
(Hopoff zone la-gk)	Any call specifying this technology prefix should be directed to hop off in the la-gk zone, no matter what the area code of the called number is. (In this display, calls specifying technology prefix 7# are always routed to zone la-gk, regardless of the actual zone prefix in the destination address.)
Zone la-gk master gateway list	A list of all the gateways registered to la-gk with the technology prefix under which they are listed. (This display shows that gateways la-gw1 and la-gw2 have registered in zone la-gk with the technology prefix 7#. No priority lists are displayed here because none were defined for zone la-gk.)
(Default gateway-technology)	If no gateway-type prefix is specified in a called number, then gateways registering with 12# are the default type to be used for the call.
(Statically-configured gateways)	Lists all IP addresses and port numbers of gateways that are incapable of supplying technology-prefix information when they register. This display shows that when gateways 1.1.1.1:1720 and 2.2.2.2:1720 register, they will be considered to be of type 7#.

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call that a gatekeeper is aware of.
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.

show gatekeeper servers

To see a list of currently registered and statically configured triggers on this gatekeeper router, enter the **show gatekeeper servers** command in EXEC mode.

show gatekeeper servers [*gkid*]

Syntax Description

gkid	(Optional) The local gatekeeper name to which this trigger applies.

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2500 series, Cisco 2600 series, Cisco 3600 series, and Cisco 7200 series routers and on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

Enter this command to show all server triggers (whether dynamically registered from the external servers or statically configured from the command line interface) on this gatekeeper. If *gkid* is specified, only triggers applied to the specified gatekeeper zone appear. If the *gkid* argument is not specified, server triggers for all local gatekeeper zones on this router appear.

Examples

This example shows the operating information of the specified gk102 server:

```
Router# show gatekeeper servers gk102

                GATEKEEPER SERVERS STATUS
                =========================

     Gatekeeper Server listening port:20000

     Gatekeeper-ID:gk102
     --------------------
     RRQ  Priority:1
       Server-ID:sj-server
       Server IP address:1.14.93.28:42387
       Server type:dynamically registered
       Connection Status:active
       Trigger Information:
         Supported Prefix:10#
         Supported Prefix:3#
     RRQ  Priority:2
       Server-ID:sf-server
       Server IP address:1.14.93.43:3820
       Server type:CLI-configured
       Connection Status:inactive
       Trigger Information:
         Endpoint-type:MCU
         Endpoint-type:VOIP-GW
         Supported Prefix:99#
```

```
ARQ  Priority:1
  Server-ID:sj-server
  Server IP address:1.14.93.28:42387
  Server type:dynamically registered
  Connection Status:active
  Trigger Information:
    Destination Info:M:nilkant@zone14.com
    Destination Info:E:1800.......
    Redirect Reason:Call forwarded no reply
    Redirect Reason:Call deflection
```

Related Commands

Command	Description
debug gatekeeper server	Traces all the message exchanges between the Cisco IOS gatekeeper and the external applications. Shows any errors that occur in sending messages to the external applications or in parsing messages from the external applications.

show gatekeeper status

To show overall gatekeeper status, including authorization and authentication status, zone status, and so on, use the **show gatekeeper status** command in EXEC mode.

show gatekeeper status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command introduced in Cisco IOS Release 11.3(2)NA was integrated into Cisco IOS Release 12.0(3)T.

Examples

The following is sample output from the **show gatekeeper status** command:

```
Router# show gatekeeper status

Gatekeeper State: UP
Zone Name: gk-px4.cisco.com
Accounting: DISABLED
Security: DISABLED
```

Table 42 describes the significant fields shown in the display.

Table 42 show gatekeeper status Field Descriptions

Field	Description
Gatekeeper State	Gatekeeper status has the following values: • UP is operational. • DOWN is administratively shut down. • INACTIVE is administratively enabled, that is, the **no shutdown** command has been issued, but no local zones have been configured. • HSRP STANDBY indicates that the gatekeeper is on hot standby and will take over when the currently active gatekeeper fails.
Zone Name	Zone name.
Accounting	Authorization and accounting status.
Security	Security status.

show gatekeeper zone prefix

To display the zone prefix table, use the **show gatekeeper zone prefix** command in privileged EXEC mode.

show gatekeeper zone prefix

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.

Examples

The following is an example of output from the **show gatekeeper zone prefix** command:

```
Router# show gatekeeper zone prefix

      ZONE PREFIX TABLE
      =================
GK-NAME               E164-PREFIX
-------               -----------
gk.zone13             212.......
gk.zone14             415.......
gk.zone14             408.......
```

Table 43 describes the significant fields shown in the display.

Table 43 show gatekeeper zone prefix Field Descriptions

Field	Description
GK-NAME	Gatekeeper name.
E164-PREFIX	The E.164 prefix and a dot that acts as a wildcard for matching each remaining number in the telephone number.

show gatekeeper zone status

To display the status of zones related to a gatekeeper, use the **show gatekeeper zone status** command in privileged EXEC mode.

show gatekeeper zone status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
12.0(5)T	This display format was modified for H.323 Version 2.

Usage Guidelines

Use this command to display the status of all zones related to a gatekeeper.

Examples

The following is an example of output from the **show gatekeeper zone status** command:

```
Router# show gatekeeper zone status

                      GATEKEEPER ZONES
                      ================
GK name      Domain Name   RAS Address     PORT  FLAGS MAX-BW   CUR-BW
                                                        (kbps)   (kbps)
-------      -----------   -----------     ----  ----- ------   ------
sj.xyz.com   xyz.com       1.14.93.85      1719  LS             0
  SUBNET ATTRIBUTES :
    All Other Subnets :(Enabled)
  PROXY USAGE CONFIGURATION :
    inbound Calls from germany.xyz.com :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to germany.xyz.com
      from terminals in local zone germany.xyz.com :use proxy
      from gateways in local zone germany.xyz.com  :do not use proxy
    Inbound Calls from all other zones :
      to terminals in local zone sj.xyz.com :use proxy
      to gateways in local zone sj.xyz.com  :do not use proxy
    Outbound Calls to all other zones :
      from terminals in local zone sj.xyz.com :do not use proxy
      from gateways in local zone sj.xyz.com  :do not use proxy
tokyo.xyz.co xyz.com       172.21.139.89      1719  RS             0
milan.xyz.co xyz.com       171.69.57.90       1719  RS             0
```

Table 44 describes the significant fields shown in the display.

Table 44 show gatekeeper zone status Field Descriptions

Field	Description
GK name	The gatekeeper name (also known as zone name), which is truncated after 12 characters in the display.
Domain Name	The domain with which the gatekeeper is associated.
RAS Address	The registration, admission, and status (RAS) protocol address of the gatekeeper.
FLAGS	Displays the following information: • S = static (CLI-configured, not DNS-discovered) • L = local • R = remote
MAX-BW	The maximum bandwidth for the zone, in kbps.
CUR-BW	The current bandwidth in use, in kbps.
SUBNET ATTRIBUTES	A list of subnets controlled by the local gatekeeper.
PROXY USAGE CONFIGURATION	Inbound and outbound proxy policies as configured for the local gatekeeper (or zone).

Related Commands

Command	Description
show gatekeeper calls	Displays the status of each ongoing call of which a gatekeeper is aware.
show gatekeeper endpoints	Displays the status of all registered endpoints for a gatekeeper.
show gateway	Displays the current gateway status.

show gateway

To display the current gateway status, use the **show gateway** command in privileged EXEC mode.

show gateway

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(6)NA2	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers.
12.0(5)T	This display format was modified for H.323 V2.

Usage Guidelines

This command displays the current gateway status.

Examples

The following example shows the report that appears when the gateway is not registered with a gatekeeper:

```
Router# show gateway

Gateway gateway1 is not registered to any gatekeeper
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Enabled but NOT Active
H323 resource threshold values:
    DSP: Low threshold 60, High threshold 70
    DS0: Low threshold 60, High threshold 70
```

This following example indicates that an E.164 address has been assigned to the gateway:

```
Router# show gate

Gateway  gateway1 is registered to Gatekeeper gk1
Gateway alias list
E.164 Number 5551212
H323-ID gateway1
```

The following example shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is enabled with the **resource threshold** command:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
```

```
H323-ID gateway1
H323 resource thresholding is Enabled and Active
H323 resource threshold values:
    DSP: Low threshold 60, High threshold 70
    DS0: Low threshold 60, High threshold 70
```

The following example shows the report that appears when the gateway is registered with a gatekeeper and H.323 resource threshold reporting is disabled with the **no resource threshold** command:

```
Router# show gateway

Gateway gateway1 is registered to Gatekeeper gk1
Gateway alias list
H323-ID gateway1
H323 resource thresholding is Disabled
```

Related Commands

Command	Description
resource threshold	Configures a gateway to report H.323 resource availability to the gatekeeper of the gateway.

show interface dspfarm

To display digital signal processor (DSP) information on the two-port T1/E1 high-density port adapter for the Cisco 7200 series, use the **show interface dspfarm** command in privileged EXEC mode.

show interface dspfarm [*slot/port*]

Syntax Description

slot	(Optional) Slot location of the port adapter.
/port	(Optional) Port number on the port adapter.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series router.
12.1(1)T	This command was integrated into the Cisco IOS 12.1(1)T.

Usage Guidelines

The local time-division multiplexing (TDM) cross-connect map can be displayed.

Examples

The following example is sample output from the show interface dspfarm command for port adapter slot 0 of chassis slot 3, on the Cisco 7200 series router:

```
Router# show interface dspfarm 3/0

DSPfarm3/0 is up, line protocol is up
  Hardware is VXC-2T1/E1
  MTU 256 bytes, BW 12000 Kbit, DLY 0 usec,
     reliability 255/255, txload 4/255, rxload 1/255
  Encapsulation VOICE, loopback not set
  C549 DSP Firmware Version:MajorRelease.MinorRelease (BuildNumber)
     DSP Boot Loader:255.255 (255)
     DSP Application:4.0 (3)
     Medium Complexity Application:3.2 (5)
     High Complexity Application:3.2 (5)
  Total DSPs 30, DSP0-DSP29, Jukebox DSP id 30
  Down DSPs:none
  Total sig channels 120 used 24, total voice channels 120 used 0
     0 active calls, 0 max active calls, 0 total calls
     30887 rx packets, 0 rx drops, 30921 tx packets, 0 tx frags
     0 curr_dsp_tx_queued, 29 max_dsp_tx_queued
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Queueing strategy:fifo
  Output queue 0/0, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 13000 bits/sec, 94 packets/sec
  5 minute output rate 193000 bits/sec, 94 packets/sec
```

```
30887 packets input, 616516 bytes, 0 no buffer
Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
30921 packets output, 7868892 bytes, 0 underruns
0 output errors, 0 collisions, 0 interface resets
0 output buffer failures, 0 output buffers swapped out
```

Table 45 describes the significant fields shown in the display.

Table 45 show interface dspfarm Field Descriptions

Field	Description
DSPfarm3/0 is up	DSPfarm interface is operating. The interface state can be up, down, or administratively down.
Line protocol is	Indicates whether the software processes that handle the line protocol consider the line usable or if it has been taken down by an administrator.
Hardware	Version number of the hardware.
MTU	256 bytes.
BW	12000 Kbit.
DLY	Delay of the interface in microseconds.
Reliability	Reliability of the interface as a fraction of 255 (255/255 is 100% reliability, calculated as an expediential average over 5 minutes).
Txload	Number of packets sent.
Rxload	Number of packets received.
Encapsulation	Encapsulation method assigned to the interface.
Loopback	Loopback conditions.
C549 DSP Firmware Version	The version of DSP firmware installed.
DSP Boot Loader	DSP boot loader version.
DSP Application	DSP application code version.
Medium Complexity Application	DSP Medium Complexity Application code version.
High Complexity Application	DSP High Complexity Application code version.
Total DSPs	Total DSPs that are equipped in the PA.
DSP0-DSP	DSP number range.
Jukebox DSP id	Jukebox DSP number.
Down DSPs	DSPs not in service.
Total sig channels...used...	Total number of signal channels used.
Total voice channels...used...	Total number of voice channels used.
Active calls	Number of active calls.
Max active calls	Maximum number of active calls.
Total calls	Total number of calls.
Rx packets	Number of received (rx) packets.
Rx drops	Number of rx packets dropped at PA.

Table 45 show interface dspfarm Field Descriptions (continued)

Field	Description
Tx packets	Number of transmit (tx) packets.
Tx frags	Number of tx packets that were fragmented.
Curr_dsp_tx_queued	Number of tx packets that are being queued at host DSP queues.
Max_dsp_tx_queued	The max total tx packets that were queued at host DSP queues.
Last input	Number of hours, minutes, and seconds since the last packet was successfully received by an interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output	Number of hours, minutes, and seconds since the last packet was successfully sent by the interface. Useful for knowing when a dead interface failed. This counter is updated only when packets are process switched and not when packets are fast switched.
Output hang	Number of hours, minutes, and seconds (or never) since the interface was last reset because of a transmission that took too long. When the number of hours in any of the “last” fields exceeds 24 hours, the number of days and hours is printed. If that field overflows, asterisks (**) are printed.
Last clearing of “show interface” counters	Number of times the “show interface” counters were cleared.
queueing strategy	First-in, first-out queueing strategy (other queueing strategies you might see are priority-list, custom-list, and weighted fair).
Output queue	Number of packets in output queue.
Drops	Number of packets dropped because of a full queue.
Input queue	Number of packets in input queue.
Minute input rate	Average number of bits and packets received per minute in the past 5 minutes.
Bits/sec	Average number of bits sent per second.
Packets/sec	Average number of packets sent per second.
Packets input	Total number of error-free packets received by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, in the error free packets received by the system.
No buffer	Number of received packets discarded because there was no buffer space in the main system. Compare with ignored count. Broadcast storms on Ethernets and bursts of noise on serial lines are often responsible for no-input-buffer events.
Received...broadcasts	Total number of broadcast or multicast packets received by the interface.
Runts	Number of packets that are discarded because they are smaller than the minimum packet size for the medium. For instance, any Ethernet packet that is less than 64 bytes is considered a runt.

Table 45 show interface dspfarm Field Descriptions (continued)

Field	Description
Giants	Number of packets that are discarded because they exceed the maximum packet size for the medium. For instance, any Ethernet packet that is greater than 1518 bytes is considered a giant.
Throttles	Number of times the receiver on the port was disabled, possibly because of buffer or processor overload.
Input errors	Number of packet input errors.
CRC	Cyclic redundancy checksum generated by the originating LAN station or far end device does not match the checksum calculated from the data received. On a LAN, this usually indicates noise or transmission problems on the LAN interface or the LAN bus itself. A high number of CRCs is usually the result of collisions or a station sending bad data. On a serial link, CRCs usually indicate noise, gain hits, or other transmission problems on the data link.
Frame	Number of packets received incorrectly having a CRC error and a noninteger number of octets. On a serial line, this is usually the result of noise or other transmission problems.
Overrun	Number of times the serial receiver hardware was unable to hand received data to a hardware buffer because the input rate exceeded the ability of the receiver to handle the data.
Ignore	Number of received packets ignored by the interface because the interface hardware ran low on internal buffers. These buffers are different from the system buffers mentioned previously in the buffer description. Broadcast storms and bursts of noise can cause the ignored count to be incremented.
Abort	Illegal sequence of one bits on the interface.
Packets output	Total number of messages sent by the system.
Bytes	Total number of bytes, including data and MAC encapsulation, sent by the system.
Underruns	Number of times that the far end transmitter has been running faster than the near-end router's receiver can handle.
Output errors	Sum of all errors that prevented the final transmission of datagrams out of the interface being examined. Note that this value might not balance with the sum of the enumerated output errors; some datagrams can have more than one error, and others can have errors that do not fall into any of the specifically tabulated categories.
Collisions	Number of messages re-sent because of an Ethernet collision. Collisions are usually the result of an overextended LAN (Ethernet or transceiver cable too long, more than two repeaters between stations, or too many cascaded multiport transceivers). A packet that collides is counted only once in output packets.

Table 45 show interface dspfarm Field Descriptions (continued)

Field	Description
Interface resets	Number of times an interface has been completely reset. Resetting can happen if packets queued for transmission were not sent within a certain interval. If the system notices that the carrier detect line of an interface is up, but the line protocol is down, it periodically resets the interface in an effort to restart it. Interface resets can also occur when an unrecoverable interface processor error occurs, or when an interface is looped back or shut down.
Output buffer failures	Number of failed buffers.
Output buffers swapped out	Number of buffers swapped out.

show mgcp

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp** command in EXEC mode.

show mgcp

Defaults

No defaults

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Output was updated to show additional gateway and platform information.

Examples

The following displays an example of the command format and output for **show mgcp**.

```
Router# show mgcp

MGCP Admin State ACTIVE, Oper State ACTIVE - Cause Code NONE
MGCP call-agent: 192.168.10.10 2302 Initial protocol service is MGCP
mgcp block-newcalls DISABLED
MGCP dtmf-relay disabled for all codec types
MGCP modem passthru: CA
MGCP request timeout 500, MGCP request retries 3
MGCP gateway port: 2427, MGCP maximum waiting delay 3000
MGCP restart delay 5, MGCP vad DISABLED
MGCP sdp simple DISABLED, MGCP cisco fgdos DISABLED
MGCP codec type g711ulaw, MGCP packetization period 20
MGCP JB threshold lwm 30, MGCP JB threshold hwm 150
MGCP LAT threshold lwm 150, MGCP LAT threshold hwm 300
MGCP PL threshold lwm 1000, MGCP PL threshold hwm 10000
MGCP playout mode is adaptive 60, 4, 200 in msec
MGCP IP ToS low delay disabled, MGCP IP ToS high throughput disabled
MGCP IP ToS high reliability disabled, MGCP IP ToS low cost disabled
MGCP IP precedence 3, MGCP default package: trunk-package
MGCP supported packages: gm-package dtmf-package trunk-package rtp-package
as-packagescript-package
```

Table 46 describes the significant fields shown in the display.

Table 46 show mgcp Field Descriptions

MGCP Admin State...Oper State	The administrative and operational state of the MGCP daemon. The administrative state controls starting and stopping the application using the **mgcp** and **mgcp block-newcalls** commands. The operational state controls normal MGCP operations.
MGCP call-agent	The address of the call agent specified in the **mgcp** command.
Initial protocol service is...	Indicates the protocol initiated for this session.
MGCP block-newcalls enabled	The state of the **mgcp block-newcalls** command.
MGCP dtmf-relay	The setting for the **mgcp dtmf-relay** command.
MGCP modem passthru	Indicates whether a call agent will be involved in relaying modem data.
MGCP request timeout	The setting for the **mgcp request timeout** command.
MGCP request retries	The setting for the **mgcp request retries** command.
MGCP gateway port	The UDP port specification.
MGCP maximum waiting delay	The setting for the **mgcp max-waiting-delay** command.
MGCP restart delay	The setting for the **mgcp restart-delay** command.
MGCP vad	The setting for the **mgcp vad** command.
MGCP sdp simple	Indicates whether the simple sdp protocol is being used.
MGCP cisco fgdos	For Cisco use only.
MGCP codec type	The setting for the **mgcp codec** command.
MGCP packetization period	The **packetization period** parameter setting for the **mgcp codec** command.
MGCP JB threshold lwm	The jitter buffer minimum threshold parameter setting for the **mgcp quality-threshold** command.
MGCP JB threshold hwm	The jitter buffer maximum threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold lwm	The latency minimum threshold parameter setting for the **mgcp quality-threshold** command.
MGCP LAT threshold hwm	The latency maximum threshold parameter setting for the **mgcp quality-threshold** command.
MGCP PL threshold lwm	The packet loss minimum threshold parameter setting for the **mgcp quality-threshold** command.
MGCP PL threshold hwm	The packet loss maximum threshold parameter setting for the **mgcp quality-threshold** command.
MGCP playout mode	The jitter buffer packet size type and size.
MGCP IP ToS low delay	The **low-delay** parameter setting for the **mgcp ip-tos** command.
MGCP IP ToS high throughput	The **high-throughput** parameter setting for the **mgcp ip-tos** command.

Table 46 show mgcp Field Descriptions (continued)

MGCP IP ToS high reliability	The **high-reliability** parameter setting for the **mgcp ip-tos** command.
MGCP IP ToS low cost	The **low-cost** parameter setting for the **mgcp ip-tos** command.
MGCP IP precedence	The **precedence** parameter setting for the **mgcp ip-tos** command.
MGCP default package	The default-package parameter setting for the **mgcp default-package** command.
MGCP supported packages	The packages supported in this session.

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp connection	Displays connection-related MGCP configuration information.
show mgcp endpoint	Displays endpoint-specific MGCP configuration information.
show mgcp statistics	Displays statistical MGCP configuration information.

show mgcp connection

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp connection** command in EXEC mode.

show mgcp connection

Syntax Description

connection	Displays the active MGCP-controlled connections.

Defaults

No defaults

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Output was updated to show additional gateway and platform information.

Examples

Following is an example of an MGCP configuration displaying active MGCP-controlled connections.

```
Router# show mgcp connection

Endpoint   Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (C)odec (E)vent[SIFL] (R)esult[EA]
1. S0/DS1-0/1 C=103,23,24 I=0x8 P=16586,16634 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
2. S0/DS1-0/2 C=103,25,26 I=0x9 P=16634,16586 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
3. S0/DS1-0/3 C=101,15,16 I=0x4 P=16506,16544 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
4. S0/DS1-0/4 C=101,17,18 I=0x5 P=16544,16506 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0
5. S0/DS1-0/5 C=102,19,20 I=0,6 P=16572,16600 M=3 S=4,4 C=5 E=2,0,0,2 R=0,0
6. S0/DS1-0/6 C=102,21,22 I=0x7 P=16600,16572 M=3 S=4,4 C=5 E=0,0,0,0 R=0,0

Total number of active calls 6
```

Table 47 describes the significant fields shown in the display.

Table 47 show mgcp connection Field Descriptions

Endpoint	The endpoint for each call shown in the digital endpoint naming convention of slot number (S0) and digital line (DS1-0) number (1).
Call_ID(C)	The MGCP call ID sent by the call agent, the internal Call Control Application Programming Interface (CCAPI) call ID for this endpoint, and the peer call legs CCAPI call ID. (CCAPI is an API that provides call control facilities to applications.)
Conn_ID(I)	The connection ID generated by the gateway and sent in the ACK message.

Table 47 show mgcp connection Field Descriptions (continued)

(P)ort	The ports used for this connection. The first port is the local UDP port. The second port is the remote UDP port.
(M)ode	The call mode, where: 0—An invalid value for mode. 1—The gateway should only send packets. 2—The gateway should only receive packets. 3—The gateway can send and receive packets. 4—The gateway should neither send nor receive packets. 5—The gateway should place the circuit in loopback mode. 6—The gateway should place the circuit in test mode. 7—The gateway should use the circuit for network access for data. 8—The gateway should place the connection in network loopback mode. 9—The gateway should place the connection in network continuity test mode. 10— The gateway should place the connection in conference mode. All other values are used for internal debugging.
(S)tate	The call state. The values are used for internal debugging purposes.
(C)odec	The codec identifier. The values are used for internal debugging purposes.
(E)vent [SIFL]	Used for internal debugging.
(R)esult [EA]	Used for internal debugging.

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp	Displays general MGCP configuration information.
show mgcp endpoint	Displays endpoint-specific MGCP configuration information.
show mgcp statistics	Displays statistical MGCP configuration information.

show mgcp endpoint

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp endpoint** command in EXEC mode.

show mgcp endpoint

Syntax Description

endpoint	Displays the MGCP-controlled endpoints.

Defaults

No defaults

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Output was updated to show additional gateway and platform information.

Examples

The following example shows how endpoints are configured:

```
Router# show mgcp endpoint

T1/0 ds0-group 0 timeslots 1-24 type none
T1/1 ds0-group 0 timeslots 1-24 type none
T1/2 ds0-group 0 timeslots 1-24 type none
T1/3 ds0-group 0 timeslots 1-24 type none
```

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp	Displays general MGCP configuration information.
show mgcp connection	Displays connection-related MGCP configuration information.
show mgcp statistics	Displays statistical MGCP configuration information.

show mgcp statistics

To display Media Gateway Control Protocol (MGCP) configuration information, use the **show mgcp statistics** command in EXEC mode.

show mgcp statistics

Syntax Description

statistics	Displays MGCP statistics regarding network messages that have been received and sent.

Defaults

No defaults

Command Modes

EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced for the Cisco AS5300 universal access server.
12.1(3)T	Output was updated to show additional gateway and platform information.

Examples

Following is an example of an MGCP configuration displaying MGCP statistics of network messages that have been received and sent.

```
Router# show mgcp statistics

UDP pkts rx 8, tx 9
Unrecognized rx pkts 0, MGCP message parsing errors 0
Duplicate MGCP ack tx 0, Invalid versions count 0
CreateConn rx 4, successful 0, failed 0
DeleteConn rx 2, successful 2, failed 0
ModifyConn rx 4, successful 4, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 4, failed 0
AuditConnection rx 0, successful 0, failed 0
AuditEndpoint rx 0, successful 0, failed 0
RestartInProgress tx 1, successful 1, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 8, NACK tx 0
ACK rx 0, NACK rx 0
IP address based Call Agents statistics:
IP address 10.24.167.3, Total msg rx 8, successful 8, failed 0
```

Table 48 describes the significant fields shown in the display.

Table 48 show mgcp statistics Field Descriptions

UDP pkts rx, tx	The number of UDP packets transmitted and received by the gateway's MGCP application from the Call Agent.
Unrecognized rx pkts	The number of unrecognized UDP packets received by the MGCP application.
MGCP message parsing errors	The number of MGCP messages received with parsing errors.
Duplicate MGCP ack tx messages	The number of duplicate MGCP acknowledgment messages transmitted to the Call Agent.
Invalid versions count	The number of MGCP messages received with invalid MGCP protocols version.
CreateConn rx	The number of Create Connection (CRCX) messages received by the gateway, the number that were successful, and the number that failed.
DeleteConn rx	The number of Delete Connection (DLCX) messages received by the gateway, the number that were successful, and the number that failed.
NotifyRequest rx	The number of Notify Request (RQNT) messages received by the gateway, the number that were successful, and the number that failed.
AuditConnection rx	The number of Audit Connection (AUCX) message received by the gateway, the number that were successful, and the number that failed.
AuditEndpoint rx	The number of Audit Endpoint (AUEP) messages received by the gateway, the number that were successful, and the number that failed.
RestartinProgress tx	The number of Restart in Progress (RSIP) messages transmitted by the gateway, the number that were successful, and the number that failed.
Notify tx	The number of Notify (NTFY) messages transmitted by the gateway, the number that were successful, and the number that failed.
ACK tx, NACK tx	The number of Acknowledgment and Negative Acknowledgment messages transmitted by the gateway.
ACK rx, NACK rx	The number of Acknowledgment and Negative Acknowledgment messages received by the gateway.
IP address based Call Agents statistics: IP address, Total msg rx	IP address of the Call Agent, the total number of MGCP messages received from that Call Agent, the number of messages that were successful, and the number of messages that failed.

Related Commands

Command	Description
mgcp	Starts the MGCP daemon.
show mgcp	Displays general MGCP configuration information.

show mgcp connection	Displays connection-related MGCP configuration information.
show mgcp endpoint	Displays endpoint-specific MGCP configuration information.

show num-exp

To show the number expansions configured, use the **show num-exp** command in privileged EXEC mode.

show num-exp [*dialed-number*]

Syntax Description

dialed-number	(Optional) Dialed number.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 platform.
12.0(3)T	This command was supported on the Cisco AS5300 universal access server platform.
12.0(4)XL	This command was supported on the Cisco AS5800 platform.
12.0(7)XK	This command was supported on the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into Cisco IOS 12.1(2)T.

Usage Guidelines

Use the **show num-exp** privileged EXEC command to display all the number expansions configured for this router. To display number expansion for only one number, specify that number by using the *dialed-number* argument.

Examples

The following is sample output from the **show num-exp** command:

```
Router# show num-exp

Dest Digit Pattern = '0...'     Translation = '+14085270...'
Dest Digit Pattern = '1...'     Translation = '+14085271...'
Dest Digit Pattern = '3..'      Translation = '+140852703..'
Dest Digit Pattern = '4..'      Translation = '+140852804..'
Dest Digit Pattern = '5..'      Translation = '+140852805..'
Dest Digit Pattern = '6....'    Translation = '+1408526....'
Dest Digit Pattern = '7....'    Translation = '+1408527....'
Dest Digit Pattern = '8...'     Translation = '+14085288...'
```

Table 49 describes the significant fields shown in the display.

Table 49 show num-exp Field Descriptions

Field	Description
Dest Digit Pattern	Index number identifying the destination telephone number digit pattern.
Translation	Expanded destination telephone number digit pattern.

Related Commands

Command	Description
show call active voice	Displays the Voice over IP active call table.
show call history voice	Displays the Voice over IP call history table.
show dial-peer voice	Displays configuration information for dial peers.
show voice port	Displays configuration information about a specific voice port.

show pots csm

To show the current state of calls and the most recent event received by the call switching module (CSM) on the Cisco 800 series router, use the **show pots csm** command in EXEC mode.

show pots csm *port*

Syntax Description

port	Port number 1 or 2.

Command Modes

EXEC

Command History

Release	Modification
12.1.(2)XF	This command was introduced on the Cisco 800 series routers.

Examples

The following is an example of **show pots csm** command output:

```
Router# show pots csm 1

POTS PORT: 1

   CSM Finite State Machine:
      Call 0 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 1 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
      Call 2 - State: idle, Call Id: 0x0
               Active: no
               Event: CSM_EVENT_NONE Cause: 0
```

Related Commands

Command	Description
test pots dial	Dial a telephone number for the POTS port on the router by using a dial application on your workstation.
test pots disconnect	Disconnect a telephone call for the POTS port on the router.

show pots status

To display the settings of the telephone port physical characteristics and other information on the telephone interfaces of the Cisco 800 series, use the **show pots status** command in privileged EXEC mode.

show pots status [**1** | **2**]

Syntax Description

1	(Optional) Display the settings of telephone port 1.
2	(Optional) Display the settings of telephone port 2.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco 800 series router.

Usage Guidelines

The **show pots status** command displays the settings and information for both telephone ports.

Examples

The following is sample output from the **show pots status** command.

```
Router# show pots status

POTS Global Configuration:
   Country: United States
   Dialing Method: Overlap, Tone Source: Remote, CallerId Support: YES
   Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
   Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
   Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
   TX Gain: 6dB, RX Loss: -6dB,
   Filter Mask: 6F
   Adaptive Cntrl Mask: 0
POTS PORT: 1
   Hook Switch Finite State Machine:
      State: On Hook, Event: 0
      Hook Switch Register: 10, Suspend Poll: 0
   CODEC Finite State Machine:
      State: Idle, Event: 0
      Connection: None, Call Type: Two Party, Direction: Rx only
      Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
      Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
      Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
      TX Gain: 6dB, RX Loss: -6dB,
      Filter Mask: 6F
      Adaptive Cntrl Mask: 0
```

```
    CODEC Registers:
       SPI Addr: 2, DSLAC Revision: 4
       SLIC Cmd: 0D, TX TS: 00, RX TS: 00
       Op Fn: 6F, Op Fn2: 00, Op Cond: 00
       AISN: 6D, ELT: B5, EPG: 32 52 00 00
       SLIC Pin Direction: 1F
    CODEC Coefficients:
       GX: A0 00
       GR: 3A A1
        Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
        B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
        X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
        R: 01 11 01 90 01 90 01 90 01 90 01 90
       GZ: 60
      ADAPT B: 91 B2 8F 62 31
    CSM Finite State Machine:
       Call 0 - State: idle, Call Id: 0x0
                Active: no
       Call 1 - State: idle, Call Id: 0x0
                Active: no
       Call 2 - State: idle, Call Id: 0x0
                Active: no
 POTS PORT: 2
    Hook Switch Finite State Machine:
       State: On Hook, Event: 0
       Hook Switch Register: 20, Suspend Poll: 0
    CODEC Finite State Machine:
       State: Idle, Event: 0
       Connection: None, Call Type: Two Party, Direction: Rx only
       Line Type: 600 ohm, PCM Encoding: u-law, Disc Type: OSI,
       Ringing Frequency: 20Hz, Distinctive Ring Guard timer: 0 msec
       Disconnect timer: 1000 msec, Disconnect Silence timer: 5 sec
       TX Gain: 6dB, RX Loss: -6dB,
       Filter Mask: 6F
       Adaptive Cntrl Mask: 0
    CODEC Registers:
       SPI Addr: 3, DSLAC Revision: 4
       SLIC Cmd: 0D, TX TS: 00, RX TS: 00
       Op Fn: 6F, Op Fn2: 00, Op Cond: 00
       AISN: 6D, ELT: B5, EPG: 32 52 00 00
       SLIC Pin Direction: 1F
    CODEC Coefficients:
       GX: A0 00
       GR: 3A A1
        Z: EA 23 2A 35 A5 9F C2 AD 3A AE 22 46 C2 F0
        B: 29 FA 8F 2A CB A9 23 92 2B 49 F5 37 1D 01
        X: AB 40 3B 9F A8 7E 22 97 36 A6 2A AE
        R: 01 11 01 90 01 90 01 90 01 90 01 90
       GZ: 60
      ADAPT B: 91 B2 8F 62 31
    CSM Finite State Machine:
       Call 0 - State: idle, Call Id: 0x0
                Active: no
       Call 1 - State: idle, Call Id: 0x0
                Active: no
       Call 2 - State: idle, Call Id: 0x0
                Active: no
 Time Slot Control: 0
```

Table 50 describes the significant fields shown in the display.

Table 50 show pots status Field Descriptions

Field	Descriptions
POTS Global Configuration	Displays the settings of the telephone port physical characteristic commands. Also displays the following: • TX GAIN—Current transmit gain of telephone ports. • RX LOSS—Current transmit loss of telephone ports. • Filter Mask—Value determines which filters are currently enabled or disabled in the telephone port hardware. • Adaptive Cntrl Mask—Value determines if telephone port adaptive line impedance hardware is enabled or disabled.
Hook Switch Finite State Machine	Device driver that tracks state of telephone port hook switch.
CODEC Finite State Machine	Device driver that controls telephone port codec hardware.
CODEC Registers	Register contents of telephone port codec hardware.
CODEC Coefficients	Codec coefficients selected by telephone port driver. Selected line type determines codec coefficients.
CSM Finite State Machine	State of call-switching module (CSM) software.
Time Slot Control	Register that determines if telephone port voice or data packets are sent to an ISDN B channel.

Related Commands

Command	Description
pots country	Configures telephones, fax machines, or modems connected to a Cisco 800 series router to use country-specific default settings for each physical characteristic.
pots dialing-method	Specifies how the Cisco 800 series router collects and sends digits dialed on your connected telephones, fax machines, or modems.
pots disconnect-supervision	Specifies how a Cisco 800 series router notifies the connected telephones, fax machines, or modems when the calling party has disconnected.
pots disconnect-time	Specifies the interval in which the disconnect method is applied if telephones, fax machines, or modems connected to a Cisco 800 series router fail to detect that a calling party has disconnected.
pots distinctive-ring-guard-time	Specifies a delay in which a telephone port can be rung after a previous call is disconnected (Cisco 800 series routers).
pots encoding	Specifies the PCM encoding scheme for telephones, fax machines, or modems connected to a Cisco 800 series router.
pots line-type	Specifies the impedance of telephones, fax machines, or modems connected to a Cisco 800 series router.
pots ringing-freq	Specifies the frequency at which telephones, fax machines, or modems connected to a Cisco 800 series router ring.

Command	Description
pots silence-time	Specifies the interval of silence after a calling party disconnects (Cisco 800 series router).
pots tone-source	Specifies the source of dial, ringback, and busy tones for telephones, fax machines, or modems connected to a Cisco 800 series router.

show proxy h323 calls

To list each active call on the proxy, use the **show proxy h323 calls** command in privileged EXEC mode.

show proxy h323 calls

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Examples

The following is sample output from the **show proxy h323 calls** command:

```
Router# show proxy h323 calls

Call unique key = 1
  Conference ID = [277B87C0A283D111B63E00609704D8EA]
  Calling endpoint call signalling address = 55.0.0.41
  Calling endpoint aliases:
   H323_ID: ptel11@zone1.com
  Call state = Media Streaming
  Time call was initiated = 731146290 ms
```

show proxy h323 detail-call

To display the details of a particular call on a proxy, use the **show proxy h323 detail-call** command in privileged EXEC mode.

show proxy h323 detail-call *call-key*

Syntax Description

call-key	Specifies the call you want to display. The *call-key* argument is derived from the **show proxy h323 calls** display.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

The **show proxy h323 detail-call** command can be used with or without the proxy statistics enabled.

Examples

The following is sample output from the **show proxy h323 detail-call** command without the proxy statistics enabled:

```
Router# show proxy h323 detail-call 1

ConferenceID = [277B87C0A283D111B63E00609704D8EA]
Calling endpoint aliases:
      H323_ID: ptel11@zone1.com
Called endpoint aliases:
      H323_ID: ptel21@zone2.com
Peer proxy call signalling address = 55.0.0.41
Time call was initiated = 731146290 ms
Inbound CRV = 144
Outbound CRV = 70
Call state = Media Streaming
H245 logical channels for call leg pte111@zone1.com<->px1@zone.com
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
```

```
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
H245 logical channels for call leg pte111@zone1.com<->50.0.0.41:
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146317 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146316 ms
    Channel number = 2
        Type = VIDEO
        State = OPEN
        Bandwidth = 374 kbps
        Time created = 731146318 ms
    Channel number = 1
        Type = AUDIO
        State = OPEN
        Bandwidth = 81 kbps
        Time created = 731146317 ms
```

The following is sample output from the **show proxy h323 detail-call** command with the proxy statistics enabled:

```
Router# show proxy h323 detail-call 1

ConferenceID = [677EB106BD0D111976200002424F832]
Calling endpoint call signalling address = 172.21.127.49
    Calling endpoint aliases:
      H323_ID: intel2
      E164_ID: 2134
Called endpoint aliases:
      H323_ID: mcs@sanjose.cisco.com
Peer proxy call signalling address = 171.68.183.199
Peer proxy aliases:
      H323_ID: proxy.sanjose.cisco.com
Time call was initiated = 730949651 ms
Inbound CRV = 2505
Outbound CRV = 67
Call state = H245 open logical channels
H245 logical channels for call leg intel2 <-> cisco7-pxy:
    Channel number = 259
      RTP stream from intel2 to cisco7-pxy
        Type = VIDEO
        State = OPEN
        Bandwidth = 225 kbps
        Time created = 730949676 ms
    Channel number = 257
      RTP stream from intel2 to cisco7-pxy
        Type = AUDIO
        State = OPEN
        Bandwidth = 18 kbps
        Time created = 730949658 ms
    Channel number = 2
      RTP stream from cisco7-pxy to intel2
        Type = VIDEO
```

```
State = OPEN
Bandwidth = 225 kbps
Time created = 730949664 ms
RTP Statistics:
  Packet Received Count = 3390
  Packet Dropped Count = 0
  Packet Out of Sequence Count = 0
  Number of initial packets used for Arrival-Spacing bin setup = 200
  min_arrival_spacing = 0(ms)  max_arrival_spacing = 856(ms)
  Average Arrival Rate = 86(ms)
  Arrival-Spacing(ms)   Packet-Count
     0                    2116
     26                   487
     52                   26
     78                   0
     104                  0
     130                  1
     156                  0
     182                  1
     208                  0
     234                  4
     260                  99
     286                  315
     312                  154
     338                  8
     364                  0
     390                  2
     416                  10
     442                  73
     468                  51
     494                  43
  ==============================
  Min Jitter = 34(ms)  Max Jitter = 408(ms)
  Average Jitter Rate = 117
  Jitter Rate(ms)   Packet-Count
     0                    0
     41                   514
     82                   2117
  Number of initial packets used for Arrival-Spacing bin setup = 200
  min_arrival_spacing = 32(ms)  max_arrival_spacing = 96(ms)
  Average Arrival Rate = 60(ms)
  Arrival-Spacing(ms)   Packet-Count
     32                   35
     34                   0
     36                   177
     38                   0
     40                   56
     42                    0
     44                   10
     46                   0
     48                   27
     50                   0
     52                   541
     54                   0
     56                   2642
     58                   1
     60                   1069
     62                   0
     64                   77 0
     68                   6
     70                   257
  ==============================
```

```
            Min Jitter = 0(ms)  Max Jitter = 28(ms)
            Average Jitter Rate = 5
            Jitter Rate(ms)   Packet-Count
               0                     1069
               3                     2720
               6                     0
               9                     804
               12                    27
               15                    10
               18                    0
               21                    56
               24                    177
               27                    35
  H245 logical channels for call leg cisco7-pxy <->
  proxy.sanjose.cisco.com:
      Channel number = 259
        RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
          Type = VIDEO
          State = OPEN
          Bandwidth = 225 kbps
          Time created = 730949676 ms
          RTP Statistics:
            Packet Received Count = 3398
            Packet Dropped Count = 1
            Packet Out of Sequence Count = 0
            Number of initial packets used for Arrival-Spacing bin setup = 200
            min_arrival_spacing = 0(ms)  max_arrival_spacing = 872(ms)
            Average Arrival Rate = 85(ms)
            Arrival-Spacing(ms)   Packet-Count
               0                     2636
               28                    0
               56                    0
               84                    0
               112                   0
               140                   1
               168                   0
               196                   0
               224                   0
               252                   0
               280                   2
               308                   425
               336                   154
               364                   5
               392                   0
               420                   0
               448                   0
               476                   114
               504                   41
               532                   20
            ==============================
            Min Jitter = 55(ms)  Max Jitter = 447(ms)
            Average Jitter Rate = 127
            Jitter Rate(ms)   Packet-Count
               0                     0
               45                    1
               90                    2636
               135                   0
               180                   2
               225                   425
               270                   159
               315                   0
               360                   0
               405                   175
```

```
Channel number = 257
  RTP stream from cisco7-pxy to proxy.sanjose.cisco.com
    Type = AUDIO
    State = OPEN
    Bandwidth = 18 kbps
    Time created = 730949658 ms
    RTP Statistics:
      Packet Received Count = 2537
      Packet Dropped Count = 3
      Packet Out of Sequence Count = 0
      Number of initial packets used for Arrival-Spacing bin setup = 200
      min_arrival_spacing = 0(ms)  max_arrival_spacing = 32716(ms)
      Average Arrival Rate = 112(ms)
      Arrival-Spacing(ms)   Packet-Count
         0                     2191
         72                    253
         144                   31
         216                   7
         288                   3
         360                   4
         432                   4
         504                   2
         576                   1
         648                   3
         720                   2
         792                   1
         864                   2
         936                   1
         1008                  1
         1080                  1
         1152                  1
         1224                  1
         1296                  0
         1368                  28
      ==============================
      Min Jitter = 32(ms)  Max Jitter = 1256(ms)
      Average Jitter Rate = 121
      Jitter Rate(ms)   Packet-Count
         0                     284
         126                   2201
         252                   4
         378                   6
         504                   4
         630                   3
         756                   2
         882                   2
         1008                  2
         1134                  29
Channel number = 2
  RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
    Type = VIDEO
    State = OPEN
    Bandwidth = 225 kbps
    Time created = 730949664 ms
Channel number = 1
  RTP stream from proxy.sanjose.cisco.com to cisco7-pxy
    Type = AUDIO
    State = OPEN
    Bandwidth = 18 kbps
    Time created = 730949661 ms
```

Related Commands

Command	Description
h323 qos	Enables QoS on the proxy.

show proxy h323 status

To display the overall status of a proxy, use the **show proxy h323 status** command in privileged EXEC mode.

show proxy h323 status

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(2)NA	This command was introduced.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Examples

The following is sample output from the **show proxy h323 status** command:

```
Router# show proxy h323 status

  H.323 Proxy Status
        ==================
    H.323 Proxy Mode: Enabled
    Proxy interface = Serial1: UP
    Application Specific Routing: Disabled
    RAS Initialization: Complete
    Proxy aliases configured:
      H323_ID: px2
    Proxy aliases assigned by Gatekeeper:
      H323_ID: px2
    Gatekeeper multicast discovery: Disabled
    Gatekeeper:
        Gatekeeper ID: gk.zone2.com
        IP address: 70.0.0.31
    Gatekeeper registration succeeded
    T.120 Mode: BYPASS
    RTP Statistics: OFF
    Number of calls in progress: 1
```

show rawmsg

To show the raw messages owned by the required component, use the **show rawmsg** command in privileged EXEC mode.

show rawmsg {**all** | **tsp** | **vtsp** | **ccapi** | **h323**}

Syntax Description

all	All selections below.
tsp	Telephony Service Provider subsystem.
vtsp	Voice Telephony Service Provider subsystem.
ccapi	API (Application Programming Interface) used to coordinate interaction between application and call legs (telephony or IP).
h323	H.323 subsystem.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

The number displayed for **show rawmsg all** should be zero to indicate that there are no memory leaks.

Examples

The following example shows how to display memory leaks from the telephony service provider:

```
Router# show rawmsg tsp
```

Related Commands

Command	Description
isdn protocol-emulate	Configures the Layer 2 and Layer 3 port protocol of a BRI voice port or a PRI interface to emulate NT (network) or TE (user) functionality.
isdn switch type	Configures the Cisco AS5300 universal access server PRI interface to support Q.SIG signaling.
pri-group nec-fusion	Configures your NEC PBX to support FCCS.
show cdapi	Displays the CDAPI.

show rlm group statistics

To display the network latency of the Redundant Link Manager (RLM) group, use the **show rlm group statistics** command in privileged EXEC mode.

show rlm group *group-number* **statistics**

Syntax Description

group-number	RLM group number (0 to 255).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following is sample output from the **show rlm group** *group-number* **statistics** command:

```
Router# show rlm group 1 statistics

RLM Group 1 Statistics
 Link_up:
     last time occurred at 02:45:48.724, total transition=1
     avg=00:00:00.000, max=00:00:00.000, min=00:00:00.000, latest=00:00:00.000
 Link_down:
     last time occurred at 02:42:33.724, total transition=1
     avg=00:03:15.000, max=00:03:15.000, min=00:00:00.000, latest=00:03:15.000
 Link_recovered:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Link_switched:
     last time occurred at 00:00:00.000, success=0(0%), failure=0
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
 Server_changed:
     last time occurred at 00:00:00.000 for totally 0 times
 Server Link Group[r1-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.4.1]:
     last time occurred at 02:47:15.724, success=91(62%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Open the link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:43:03.724, success=1(100%), failure=0
     avg=162.000s, max=162.000s, min=0.000s, latest=162.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.4.2]:
     last time occurred at 02:47:19.724, success=95(63%), failure=54
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
```

```
 Server Link Group[r2-server]:
  Open the link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.1(Loopback1), 10.1.5.1]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s

Open the link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:46:06.724, success=0(0%), failure=1
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s
  Echo over link [10.1.1.2(Loopback2), 10.1.5.2]:
     last time occurred at 02:47:18.724, success=0(0%), failure=85
     avg=0.000s, max=0.000s, min=0.000s, latest=0.000s

Router#
```

Table 51 describes the significant fields shown in the display.

Table 51 show rlm group statistics Field Descriptions

Field	Description
Link_up	Statistics collected when RLM group is in link up state.
total transition	Total number of transitions into a particular RLM group state.
avg	How long the average time interval lasts.
max	How long the maximum time interval lasts.
min	How long the minimum time interval lasts.
latest	How long the most recent time interval lasts.
Link_down	Statistics collected when RLM group is in the link down state.
Link_recovered	Statistics collected when RLM group is in the link recovery state.
Link_switched	Statistics collected when RLM group is in the link switching state.
Server_changed	Statistics collected for when and how many times RLM server failover happens.
Server Link Group[r1-server]	Statistics collected for those signaling links defined under a particular server link group, for example, r1-server.
Open the link	Statistics collected when a particular signaling link connection is open (broken).
Echo over link	Statistics collected when a particular signaling link connection is established.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group status

To display the status of the Redundant Link Manager (RLM) group, use the **show rlm group status** command in privileged EXEC mode.

show rlm group *group-number* **status**

Syntax Description

group-number	RLM group number (0 to 255).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following is sample output from the **show rlm group** *group-number* **status** command:

```
Router# show rlm group 1 status

RLM Group 1 Status
 User/Port: RLM_MGR/3000
 Link State: Up         Last Link Status Reported: Up
 Next tx TID: 1         Last rx TID: 0
 Server Link Group[r1-server]:
  link [10.1.1.1(Loopback1), 10.1.4.1] = socket[active]
  link [10.1.1.2(Loopback2), 10.1.4.2] = socket[standby]
 Server Link Group[r2-server]:
  link [10.1.1.1(Loopback1), 10.1.5.1] = socket[opening]
  link [10.1.1.2(Loopback2), 10.1.5.2] = socket[opening]
```

Table 52 describes the significant fields shown in the display.

Table 52 show rlm group status Field Descriptions

Field	Description
User/Port	A list of registered RLM users and the corresponding port numbers associated with them.
RLM_MGR	RLM management module.
Link State	The current RLM group’s link state for connecting to the remote end.
Last Link Status Reported	The most recent link status change is reported to RLM users.
Next tx TID	The next transaction ID for transmission.
Last rx TID	The most recent transaction ID has been received.
Server Link Group[r1-server]	The status of all signaling links configured under a particular RLM server link group r1-server.

Table 52 show rlm group status Field Descriptions (continued)

Field	Description
socket	The status of the individual signaling link.
Server Link Group[r2-server]	The status of all signaling links configured under a particular RLM server link group (r2-server).

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

show rlm group timer

To display the current timer values, use the **show rlm group timer** command in privileged EXEC mode.

show rlm group *group-number* **timer**

Syntax Description

group-number	RLM group number (0 to 255).

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(7)	This command was introduced.

Examples

The following is sample output from the **show rlm group** *group-number* **timer** command:

```
Router# show rlm group 1 timer

RLM Group 1 Timer Values
 open_wait  = 3s               force-down  = 30s
 recovery   = 12s              switch-link = 5s
 minimum-up = 60s              retransmit  = 1s
 keepalive  = 1s
```

Table 90 describes the significant fields shown in the display.

Table 53 show rlm group timer Field Descriptions

Field	Description
open_wait	Wait for the connection request to be acknowledged.
recovery	Time to allow the link to recover to backup link before declaring the link is down.
minimum-up	Minimum time to force RLM to stay in the down state to make sure the remote end detects the link state is down.
keepalive	A keepalive packet will be sent out from network access server to CSC periodically.
force-down	Minimum time to force RLM to stay in the down state to make sure that the remote end detects that the link state is down.
switch-link	The maximum transition period allows RLM to switch from a lower preference link to a higher preference link. If the switching link does not complete successfully before this timer expires, RLM will go into the recovery state.
retransmit	Because RLM is operating under UDP, it needs to resend the control packet if the packet is not acknowledged within this retransmit interval.

Related Commands

Command	Description
clear interface	Resets the hardware logic on an interface.
clear rlm group	Clears all RLM group time stamps to zero.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group status	Displays the status of the RLM group.
shutdown (RLM)	Shuts down all of the links under the RLM group.
timer	Overwrites the default setting of timeout values.

show rtsp client session

To display cumulative information about Real Time Streaming Protocol (RTSP) session records, use the **show rtsp client session** command in privileged EXEC mode. To set the value to the default, use the **no** form of this command.

show rtsp client session {**history** | **active**} [**detailed**]

no show rtsp client session {**history** | **active**} [**detailed**]

Syntax Description

history	Displays cumulative information about the session, packet statistics, and general call information such as call ID, session ID, individual RTSP stream URLs, packet statistics, and play duration.
active	If the keyword **detailed** is not specified, the command displays the session information and stream information for the stream that is currently active.
detailed	(Optional) If the keyword **detailed** is specified, the command displays the session information and stream information in detail for all streams that are associated with the session.

Defaults

Active (current) stream information is displayed.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(3)T	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use this command to display cumulative information about the session, packet statistics, and general call information such as call ID, session ID, and so on.

Note Session refers to a session between the application and the RTSP client. Each call leg that is configured to use RTSP streaming has a session.

A call leg could play several prompts in a session; the "Play Time" refers to the play time associated with a stream or, in other words, a prompt; the cumulative play time is the sum total of all streams (or prompts) played out in a session.

The command output is a stream block that contains information about the stream (URL, packet statistics, current state of the stream, play duration, call ID, session ID, individual RTSP stream URLs, and packet statistics).

Examples

The following output is displayed when the **show rtsp client session active** command is used during an active session:

```
Router# show rtsp client session active

RTSP Session ID:0x8     Current Status:RTSP_STATUS_PLAYING
Associated CallID:0xF
Active Request:RTSP_API_REQ_PLAY
Control Protocol:TCP     Data Protocol:RTP

Total Packets Transmitted:0 (0 bytes)
Total Packets Received:708 (226560 bytes)

Cumulative Elapsed Play   Time:00:00:28.296
Cumulative Elapsed Record Time:00:00:00.000

        Session ID:0x8     State:ACTIVE
        Local  IP Address:1.13.79.45     Local  Port 16660
        Server IP Address:1.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0

        Packets Transmitted:0 (0 bytes)
        Packets Received:708 (226560 bytes)

        Elapsed Play   Time:00:00:28.296
        Elapsed  Record Time:00:00:00.000
        ReceiveDelay:85     LostPackets:0
```

The following output is displayed when the **show rtsp client session history detailed** command is used:

```
Router# show rtsp client session history detailed

RTSP Session ID:0x8
Associated CallID:0xF
Control Protocol:TCP     Data Protocol:RTP

Total Packets Transmitted:0 (0 bytes)
Total Packets Received:2398 (767360 bytes)

Cumulative Elapsed Play   Time:00:01:35.916
Cumulative Elapsed Record Time:00:00:00.000

        Session ID:0x8     State:INACTIVE
        Local  IP Address:1.13.79.45     Local  Port 16660
        Server IP Address:1.13.79.6     Server Port 11046
        Stream URL:rtsp://rtsp-cisco.cisco.com:554/chinna.au/streamid=0

        Packets Transmitted:0 (0 bytes)
        Packets Received:2398 (767360 bytes)

        Play   Time:00:01:35.916
        Record Time:00:00:00.000
        OntimeRcvPlayout:93650
        GapFillWithSilence:0
        GapFillWithPrediction:70
        GapFillWithInterpolation:0
        GapFillWithRedundancy:0
        HighWaterPlayoutDelay:85
        LoWaterPlayoutDelay:64
        ReceiveDelay:85     LostPackets:0
        EarlyPackets:2     LatePackets:12
```

Related Commands

Command	Description
rtsp client session history duration	Specifies the length of time the RTSP is kept during the session.
rtsp client session history records	Specifies the number of RTSP client session history records during the session.

show rudpv0 failures

To show SS7 Reliable User Datagram Protocol (RUDP) failure statistics, enter the **show rudpv0 failures** command in privileged EXEC mode.

show rudpv0 failures

Syntax Description

There are no keywords or arguments.

Defaults

There are no default behaviors or values.

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following example shows the display of RUDP failures. The fields are self-explanatory.

```
 show rudpv0 failures

**** RUDP Failure Stats ****

CreateBufHdrsFailure        0
CreateConnRecsFailure       0
CreateEventsFailure         0

NotReadyFailures            0
OptionNotSupportedFailures  0
OptionRequiredFailures      0
GetConnRecFailures          0
InvalidConnFailures         0
EventUnavailFailures        0

EmptyBufferSendFailures     0
BufferTooLargeFailures      0
ConnNotOpenFailures         0
SendWindowFullFailures      0
GetBufHdrSendFailures       0

GetDataBufFailures          0
GetBufHdrFailures           0

SendEackFailures            0
SendAckFailures             0
SendSynFailures             0
SendRstFailures             0
SendNullFailures            0

TimerNullFailures           0
FailedRetransmits           0
IncomingPktsDropped         0
UnknownRudpEvents           0
```

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by **show rudpv0 failures** to 0.
show rudpv0 statistics	Displays RUDP information about number of packets sent, received, and so forth. **clear rudpv0 statistics** resets the counters for these statistics to 0.

show rudpv0 statistics

To show SS7 Reliable User Datagram Protocol (RUDP) internal statistics, enter the **show rudpv0 statistics** privileged EXEC command.

show rudpv0 statistics

Syntax Description

There are no keywords or arguments.

Defaults

There are no default behaviors or values.

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Because the statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only this instance of the RUDP connection—since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the last time the **clear rudpv0 statistics** command was issued.

Examples

The following example shows the display of RUDP statistics and states for two connections. The fields are self-explanatory.

```
 show rudpv0 statistics

*** RUDP Internal Stats ****

Connection ID: 811641AC,   Current State: OPEN

RcvdInSeq                  1
RcvdOutOfSeq               0

SoftResets                 0
SoftResetsRcvd             0

TotalPacketsSent           4828
TotalPacketsReceived       4826
TotalDataBytesSent         0
TotalDataBytesReceived     4
TotalDataPacketsSent       0
TotalDataPacketsReceived   1
TotalPacketsRetrans        0
TotalPacketsDiscarded      0

Connection ID: 81163FD4,   Current State: OPEN

RcvdInSeq                  2265
RcvdOutOfSeq               0
```

```
SoftResets                 0
SoftResetsRcvd             0

TotalPacketsSent           7863
TotalPacketsReceived       6755
TotalDataBytesSent         173690
TotalDataBytesReceived     56121
TotalDataPacketsSent       2695
TotalDataPacketsReceived   2265
TotalPacketsRetrans        0
TotalPacketsDiscarded      0

Cumulative RudpV0 Statistics

RcvdInSeq                  2266
RcvdOutOfSeq               0

SoftResets                 0
SoftResetsRcvd             0

TotalPacketsSent           12691
TotalPacketsReceived       11581
TotalDataBytesSent         173690
TotalDataBytesReceived     56125
TotalDataPacketsSent       2695
TotalDataPacketsReceived   2266
TotalPacketsRetrans        0
TotalPacketsDiscarded      0
```

Related Commands

Command	Description
clear rudpv0 statistics	Resets the counters for the statistics generated by **show rudpv0 statistics** to 0.
show rudpv0 failures	Displays RUDP information about failed connections and the reasons for them. **clear rudpv0 statistics** resets the counters for these statistics to 0.

show rudpv1

To display Reliable User Datagram Protocol (RUDP) information, use the **show rudpv1** command in privileged EXEC mode.

show rudpv1 { failures | parameters | statistics }

Syntax Description

failures	RUDP failure statistics.
parameters	RUDP connection parameters.
statistics	RUDP internal statistics.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced.

Usage Guidelines

Because the statistics counters are continually updated, the cumulative total may not be exactly equal to individual connection counters. After a connection is reset, previous statistics are lost, so the current connection statistics reflect only this instance of the RUDP connection—since the last reset.

Cumulative statistics reflect counts since the router was rebooted or since the last time the **clear rudpv1 statistics** command was issued.

Examples

The following example shows sample output for **show rudpv1 failures**:

```
Router# show rudpv1 failures

**** RUDPV1 Failure Stats ****

CreateBufHdrsFailure       0
CreateConnRecsFailure      0
CreateEventQueueFailure    0
OsSpecificInitFailure      0

NotReadyFailures           0
OptionNotSupportedFailures 0
InvalidOptionFailures      0
OptionRequiredFailures     0
GetConnRecFailures         0
InvalidConnFailures        0
EventUnavailFailures       0

GetConnRecFailures         0
FindConnRecFailures        0
EmptyBufferSendFailures    0
```

```
BufferTooLargeFailures     0
ConnNotOpenFailures        0
SendWindowFullFailures     0
GetBufHdrSendFailures      0

SendInProgressFailures     0

GetDataBufFailures         0
GetBufHdrFailures          0

SendFailures               0
SendEackFailures           0
SendAckFailures            0
SendSynFailures            0
SendRstFailures            0
SendTcsFailures            0
SendNullFailures           0

TimerFailures              0
ApplQueueFailures          0
FailedRetransmits          0
IncomingPktsDropped        0
CksumErrors                0
UnknownRudpv1Events        0
InvalidVersion             0
InvalidNegotiation         0
```

The following example shows sample output for **show rudpv1 parameters**:

```
Router# show rudpv1 parameters

*** RUDPV1 Connection Parameters ***


Next Connection Id:61F72B6C,  Remote conn id 126000

  Conn State              OPEN
  Conn Type               ACTIVE
  Accept Negot params?    Yes
  Receive Window          32
  Send Window             32
  Receive Seg Size        384
  Send Seg Size           384

                      Requested     Negotiated
  Max Auto Reset          5             5
  Max Cum Ack             3             3
  Max Retrans             2             2
  Max OutOfSeq            3             3
  Cum Ack Timeout        100           100
  Retrans Timeout        300           300
  Null Seg Timeout       1000          1000
  Trans State Timeout    2000          2000
  Cksum type              Hdr           Hdr


Next Connection Id:61F72DAC,  Remote conn id 126218

  Conn State              OPEN
  Conn Type               ACTIVE
  Accept Negot params?    Yes
  Receive Window          32
  Send Window             32
  Receive Seg Size        384
```

```
  Send Seg Size          384

                   Requested     Negotiated
  Max Auto Reset         5             5
  Max Cum Ack            3             3
  Max Retrans            2             2
  Max OutOfSeq           3             3
  Cum Ack Timeout       100           100
  Retrans Timeout       300           300
  Null Seg Timeout      1000          1000
  Trans State Timeout   2000          2000
  Cksum type             Hdr           Hdr
```

The following example shows sample output for **show rudpv1 statistics**:

```
Router# show rudpv1 statistics

*** RUDPV1 Internal Stats ****

Connection ID:61F72B6C,   Current State:OPEN

RcvdInSeq                  647
RcvdOutOfSeq               95

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           1011
TotalPacketsReceived       958
TotalDataBytesSent         17808
TotalDataBytesReceived     17808
TotalDataPacketsSent       742
TotalDataPacketsReceived   742
TotalPacketsRetrans        117
TotalPacketsDiscarded      38

Connection ID:61F72DAC,   Current State:OPEN

RcvdInSeq                  0
RcvdOutOfSeq               0

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           75
TotalPacketsReceived       75
TotalDataBytesSent         0
TotalDataBytesReceived     0
TotalDataPacketsSent       0
TotalDataPacketsReceived   0
TotalPacketsRetrans        0
TotalPacketsDiscarded      0

Cumulative RudpV1 Statistics

NumCurConnections          2

RcvdInSeq                  652
RcvdOutOfSeq               95

AutoResets                 0
AutoResetsRcvd             0

TotalPacketsSent           1102
```

```
TotalPacketsReceived       1047
TotalDataBytesSent         18048
TotalDataBytesReceived     18048
TotalDataPacketsSent       752
TotalDataPacketsReceived   752
TotalPacketsRetrans        122
TotalPacketsDiscarded      38
```

Related Commands

Command	Description
clear rudpv1 statistics	Clears the RUDP statistics counters.
debug rudpv1	Displays debugging information for RUDP.

show settlement

To display the configuration for all settlement servers and see the specific provider and transactions, use the **show settlement** command in privileged EXEC mode. To reset to the default value, use the **no** form of this command.

show settlement [*provider-number* [**transactions**]]

no show settlement [*provider-number* [**transactions**]]

Syntax Description

provider-number	(Optional) Displays the attributes of a specific provider.
transactions	(Optional) Displays the transaction status of a specific provider.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(4)XH1	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following example shows information about all settlement servers configured:

```
Router# show settlement

Settlement Provider 0
Type = osp
Address url = https://1.14.115.100:6556/
Encryption = all                (default)
Max Concurrent Connections = 20 (default)
Connection Timeout = 3600 (s)   (default)
Response Timeout = 1 (s)        (default)
Retry Delay = 2 (s)             (default)
Retry Limit = 1                 (default)
Session Timeout = 86400 (s)     (default)
Customer Id = 1000
Device Id = 1000
Roaming = Disabled              (default)
Signed Token = on

Number of Connections = 0
Number of Transactions = 7
```

The following example shows transaction and state information about a specific settlement server:

```
Router# show settlement 0 transactions

Transaction ID=8796304133625270342
        state=OSPC_GET_DEST_SUCCESS, index=0
        callingNumber=5710868, calledNumber=15125551212
```

Table 54 describes the significant fields shown in the display. The provider attributes not configured are not shown.

.

Table 54 show settlement Field Descriptions

Field	Description
type	Settlement provider type.
address url	URL address of the provider.
encryption	SSL encryption method.
max-connections	Maximum number of concurrent connections to provider.
connection-timeout	Connection timeout with provider (in seconds).
response-timeout	Response timeout with provider (in seconds).
retry-delay	Delay time between retries (in seconds).
retry-limit	Number of retries.
session-timeout	SSL session timeout (in seconds).
customer-id	Customer ID, assigned by provider.
device-id	Device ID, assigned by provider.
roaming	Roaming enabled.
signed-token	Indicates if the settlement token is signed by the server.

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after a communication exchange is completed.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

show sgcp connection

To see all active SGCP connections on this router, use the **show sgcp connection** command in EXEC mode.

show sgcp connection [**interface** *number*]

Syntax Description

interface	(Optional) Specifies a DS1 interface.
number	(Optional) Specifies the T1 interface (controller) number. Valid values on the Cisco MC3810 multiservice concentrator are from 0 to 1.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines

If you do not specify an interface, this command shows all the active SGCP connections on this host. If you specify an interface, this command shows only those active connections on the specified interface.

Examples

The following example shows the active connections on this router being displayed:

```
Router# show sgcp connection

Endpoint        Call_ID(C) Conn_ID(I) (P)ort (M)ode (S)tate (E)vent[SIFL] (R)esult[EA]
1. ds1-0/1@r3810-5      C=1,1,2  I=0x1  P=16492,16476  M=3  S=4  E=3,0,0,3  R=0, 0
```

The following example shows the state of SGCP on the router being displayed:

```
Router# show sgcp connection

SGCP Admin State DOWN, Oper State DOWN
SGCP call-agent: 209.165.200.225 , SGCP graceful-shutdown enabled? FALSE
SGCP request timeout 40, SGCP request retries 10
```

Table 55 describes the significant fields shown in the display.

Table 55 show sgcp connection Field Descriptions

Field	Description
SGCP Admin State	The administrative and operational state of the SGCP daemon.
SGCP call-agent	The address of the call agent specified in the **sgcp** command.
SGCP graceful-shutdown enabled	The state of the **sgcp graceful-shutdown** command.
SGCP request timeout	The setting for the **sgcp request timeout** command.
SGCP request retries	The setting for the **sgcp request retries** command.

Related Commands

Command	Description
show sgcp endpoint	Displays SGCP endpoint information.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp endpoint

To see SGCP endpoints eligible for SGCP management, use the **show sgcp endpoint** command in EXEC mode.

show sgcp endpoint [**interface** *ds1* [*ds0*]]

Syntax Description

interface *ds1*	(Optional) Specifies the DS1 interface for which to display SGCP endpoint information. The valid range is from 1 to 1000.
ds0	(Optional) Specifies the DS0 interface for which to display SGCP endpoint information. The valid range is from 0 to 30.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.

Usage Guidelines

You can use this command to see SGCP endpoint information for the whole router, or you can see SGCP endpoint information for a specific DS1 interface and, optionally, a specific DS0. If you enter a nonexistent combination of a DS1 and DS0, the following error message appears: "No matching connection found."

Examples

The following command shows SGCP endpoint information being set for a matching connection between DS1 interface 1 and DS0 interface 10:

```
Router# show sgcp endpoint interface 1 10
```

Related Commands

Command	Description
show sgcp connection	Displays all the active connections on the host router.
show sgcp statistics	Displays global statistics for the SGCP packet count, success, and failure counts.

show sgcp statistics

To see global statistics for the SGCP packet count, success and failure counts, and other information, use the **show sgcp statistics** command in EXEC mode.

show sgcp statistics

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
12.0(7)XK	Support for this command was extended to the Cisco MC3810 multiservice concentrator and the Cisco 3600 series routers (except for the Cisco 3620) in a private release that was not generally available.
12.0(5)T	This command was introduced in a private release on the Cisco AS5300 universal access server only and was not generally available.

Examples

The following example shows SGCP packet statistics being displayed:

```
Router# show sgcp statistics

UDP pkts rx 5, tx 13
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 1, successful 1, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 3, successful 3, failed 0
Notify tx 3, successful 3, failed 0
ACK tx 4, NACK tx 0
ACK rx 1, NACK rx 0

IP address based Call Agents statistics:
IP address 1.4.63.100, Total msg rx 5,
                   successful 5, failed 2
```

The following examples show how you can filter the command return for specific information:

```
Router# show sgcp statistics | begin Failed

Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
```

```
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0
ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0

Router# show sgcp statistics | exclude ACK

UDP pkts rx 0, tx 0
Unrecognized rx pkts 0, SGCP message parsing errors 0
Duplicate SGCP ack tx 0
Failed to send SGCP messages 0
CreateConn rx 0, successful 0, failed 0
DeleteConn rx 0, successful 0, failed 0
ModifyConn rx 0, successful 0, failed 0
DeleteConn tx 0, successful 0, failed 0
NotifyRequest rx 0, successful 0, failed 0
Notify tx 0, successful 0, failed 0

Router# show sgcp statistics | include ACK

ACK tx 0, NACK tx 0
ACK rx 0, NACK rx 0
```

Related Commands

Command	Description
show sgcp connection	Display all the active connections on the host Cisco AS5300 universal access server.
show sgcp endpoint	Displays SGCP endpoint information.

show sip-ua

To display information and settings for the Session Initiation Protocol (SIP) User Agent (UA), use the **show sip-ua** command in privileged EXEC mode.

show sip-ua {**retry** | **statistics** | **status** | **timers**}

Syntax Description

retry	Displays SIP protocol retry counts.
statistics	Displays SIP UA response, traffic, and retry statistics.
status	Displays SIP UA listener status.
timers	Displays current settings for the SIP UA protocol timers.

Defaults

No default behaviors or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.1(1)T	This command was introduced on the Cisco 2600 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(3)T	The following changes were made: • The **statistics** keyword was added. • The statistics portion of the output from the **status** keyword was moved from the **status** keyword to the **statistics** keyword. • The output from the **timers** keyword was changed to reflect the changes in the **timers** command.

Examples

The following example displays output for the **show sip-ua retry** command:

```
Router# show sip-ua retry

SIP UA Retry Values
invite retry count = 2
response retry count = 2
bye retry count    = 2
cancel retry count   = 1
```

The following example displays output for the **show sip-ua statistics** command:

```
Router# show sip-ua statistics

SIP Response Statistics (Inbound/Outbound)
    Informational:
      Trying 0/0, Ringing 0/0,
      Forwarded 0/0, Queued 0/0,
      SessionProgress 0/0
    Success:
```

```
      OkInvite 0/0, OkBye 0/0,
      OkCancel 0/0, OkOptions 0/0
    Redirection (Inbound only):
      MultipleChoice 0, MovedPermanently 0,
      MovedTemporarily 0, SeeOther 0,
      UseProxy 0, AlternateService 0
    Client Error:
      BadRequest 0/0, Unauthorized 0/0,
      PaymentRequired 0/0, Forbidden 0/0,
      NotFound 0/0, MethodNotAllowed 0/0,
      NotAcceptable 0/0, ProxyAuthReqd 0/0,
      ReqTimeout 0/0, Conflict 0/0, Gone 0/0,
      LengthRequired 0/0, ReqEntityTooLarge 0/0,
      ReqURITooLarge 0/0, UnsupportedMediaType 0/0,
      BadExtension 0/0, TempNotAvailable 0/0,
      CallLegNonExistent 0/0, LoopDetected 0/0,
      TooManyHops 0/0, AddrIncomplete 0/0,
      Ambiguous 0/0, BusyHere 0/0
    Server Error:
      InternalError 0/0, NotImplemented 0/0,
      BadGateway 0/0, ServiceUnavail 0/0,
      GatewayTimeout 0/0, BadSipVer 0/0
    Global Failure:
      BusyEverywhere 0/0, Decline 0/0,
      NoExistAnywhere 0/0, NotAcceptable 0/0

SIP Total Traffic Statistics (Inbound/Outbound)
    Invite 0/0, Ack 0/0, Bye 0/0,
    Cancel 0/0, Options 0/0

Retry Statistics
    Invite 0, Bye 0, Cancel 0, Response 0
```

The following example displays output for the **show sip-ua status** command:

```
Router# show sip-ua status

SIP User Agent Status
SIP User Agent for UDP :ENABLED
SIP User Agent for TCP :ENABLED
SIP max-forwards :6
```

The following example displays output for the **show sip-ua timers** command:

```
Router# show sip-ua timers

SIP UA Timer Values (millisecs)
trying 500, expires 180000, connect 500, disconnect 500
```

Related Commands

Command	Description
sip-ua	Enables the SIP user-agent configuration commands, with which you configure the user agent.

show ss7 mtp2 ccb

To display SS7 MTP 2 Channel Control Block (CCB) information, use the **show ss7 mtp2 ccb** command in privileged EXEC mode.

show ss7 mtp2 ccb [*channel*]

Syntax Description

channel	Specifies a channel from 0 through 3.

Defaults

The default is set when you first configure the MTP 2 variant. The link must be out of service in order to change the MTP 2 variant.

If you do not specify a channel, the command shows Channel Control Block information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

The application and meaning of the output is dependent on the MTP 2 variant. For example, NTT and TTC only support emergency alignment.

Examples

The following example shows the display of MTP 2 CCB information:

```
Router# show ss7 mtp2 ccb 0
SS7 MTP2 Internal Channel Control Block Info for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
ModuloSeqNumber             = 128   (0x80  )
MaxSeqNumber                = 127   (0x7F  )
Unacked-MSUs (MaxInRTB)     = 40    (0x28  )
MaxProvingAttempts          = 5     (0x5   )
error_control               = Basic
LSSU_Len                    = 1     (0x1   )
MSU_Len                     = 272   (0x110 )

SUERM-threshold             = 64    (0x40  )
SUERM-number-octets         = 16    (0x10  )
SUERM-number-SUs            = 256   (0x100 )

Tie-AERM-Emergency          = 1     (0x1   )
Tin-AERM-Normal             = 1     (0x1   )

MSU_FISU_Accepted_flag      = FALSE
LSSU_available              = TRUE
AbnormalBSN_flag            = FALSE
```

```
AbnormalBSN_flag            = FALSE
UnreasonableBSN             = FALSE
UnreasonableFSN             = FALSE
Abnormal_FIBR_flag          = FALSE
congestionDiscard           = TRUE

ThisIsA_MSU                 = FALSE
local_processor_outage      = FALSE
remote_processor_outage     = FALSE

provingEmergencyFlag        = FALSE
RemoteProvingEmergencyFlag  = FALSE
further_proving_required    = FALSE
ForceRetransmitFlag         = FALSE
RetransmissionFlag          = FALSE

link_present                = FALSE
Debug Mask                  = 0x0
```

show ss7 mtp2 state

To display internal SS7 Message Transfer Part level 2 (MTP 2) state machine information, use the **show ss7 mtp2 state** command in privileged EXEC mode.

show ss7 mtp2 state [*channel*]

Syntax Description

channel	Specifies a channel from 0 to 3.

Defaults

If you do not specify a channel, the command shows state machine information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following examples show the display of MTP 2 state machine information for two different channels. Table 56 explains the fields.

```
Router# show ss7 mtp2 state 0
SS7 MTP2 states for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS              MTP2IAC_IDLE
  MTP2TXC_INSERVICE        MTP2RC_IDLE
  MTP2SUERM_IDLE           MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE

Router# show ss7 mtp2 state 1
SS7 MTP2 states for channel 1
Protocol version for channel 1 is Japan NTT Q.703 Version 1-1
  MTP2LSC_OOS              MTP2IAC_IDLE
  MTP2TXC_INSERVICE        MTP2RC_IDLE
  MTP2SUERM_IDLE           MTP2AERM_IDLE
  MTP2CONGESTION_IDLE
    Congestion Backhaul  = Abate
Remote Processor Outage  = FALSE
```

Table 56 SS7 MTP 2 State Information Fields

State	Description	Possible Values
MTP2LSC	Indicates the overall status of the link.	OOS—The link is Out-of-Service. INITIAL_ALIGNMENT—The link is in a transitional link alignment state. ALIGNED_READY—The link is in a transitional link alignment state. ALIGNED_NOT_READY—The link is in a transitional link alignment state. INSERVICE—The link is in service. PROCESSOR_OUTAGE—There is an outage in the local processor. This state implies that the link has been aligned. POWER_OFF—It is possible you don't have the I/O memory set to at least 40 percent. There may not be enough memory for the SS7 MTP2 signaling.
MTP2IAC	Indicates the status of the initial alignment control state machine.	IDLE—The state machine is idle. It is not aligning the link. NOT_ALIGNED—The state machine has begun the alignment process. ALIGNED— The link has exchanged the alignment handshake with the remote device. PROVING—The link alignment is being proven. This is a waiting period before the LSC state changes to INSERVICE.
MTP2TXC	Indicates the status of the transmission control state machine.	IDLE—The state machine is inactive. INSERVICE—The state machine is the active transmitter.
MTP2RC	Indicates the status of the receive control state machine.	IDLE—The state machine is inactive. INSERVICE—The state machine is the active receiver.
MTP2SUERM	Indicates the status of the signal unit error monitor (SUERM).	IDLE—The state machine is inactive. MONITORING—The SUERM is active. SUERM uses a leaky-bucket algorithm to track link errors while the link is in service. If the number of link errors reaches the threshold, the link is taken out of service.

Table 56 SS7 MTP 2 State Information Fields (continued)

State	Description	Possible Values
MTP2AERM	Indicates the status of the alignment error rate monitor state machine (AERM).	IDLE—The state machine is inactive. MONITORING—Alignment error monitor is active. This is part of the alignment process.
MTP2CONGESTION	Indicates the status of the congestion control state machine.	IDLE—The state machine is inactive. No congestion is detected; normal traffic flow. ACTIVE—Congestion has been declared. The Cisco 2600 series router is sending SIBs every T5, which indicates that the remote end should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Congestion Backhaul	Indicates congestion status of the backhaul link between the Cisco SLT and the Media Gateway Controller.	Abate—The link between the Cisco 2600 series router and the Media Gateway Controller is not under congestion. Onset—The link between the Cisco 2600 series router and the Media Gateway Controller is under congestion. and the Media Gateway Controller should stop sending new MSUs until the local Cisco 2600 series router can catch up.
Remote Processor Outage	Indicates the processor outage status of the remote.	TRUE indicates that the remote is in processor outage. FALSE indicates that the remote has not declared processor outage.

show ss7 mtp2 stats

To display SS7 MTP 2 operational statistics, use the **show ss7 mtp2 stats** command in privileged EXEC mode.

show ss7 mtp2 stats [*channel*]

Syntax Description

channel	Specifies a channel from 0 through 3.

Defaults

If you do not specify a channel, the command shows status information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following example shows operations and maintenance (OM) statistics for MTP 2 channel 0. Table 57 explains some of the fields.

```
Router# show ss7 mtp2 stats 0
SS7 MTP2 Statistics for channel 0
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
OMIACAlignAttemptCount  = 0
OMIACAlignFailCount     = 0
OMIACAlignCompleteCount = 0

OMMSU_TO_XMIT_Count     = 0
OMMSU_XMIT_Count        = 0
OMMSU_RE_XMIT_Count     = 0
OMMSU_RCV_Count         = 0
OMMSU_Posted_Count      = 0
OMMSU_too_long          = 0

OMFISU_XMIT_Count       = 0
OMFISU_RCV_Count        = 0

OMLSSU_XMIT_Count       = 17
OMLSSU_XMIT_SINCount    = 0
OMLSSU_XMIT_SIECount    = 0
OMLSSU_XMIT_SIOCount    = 0
OMLSSU_XMIT_SIOSCount   = 17
OMLSSU_XMIT_SIPOCount   = 0
OMLSSU_XMIT_SIBCount    = 0
```

```
OMLSSU_RCV_Count         = 0
OMLSSU_RCV_SINCount      = 0
OMLSSU_RCV_SIECount      = 0
OMLSSU_RCV_SIOCount      = 0
OMLSSU_RCV_SIOSCount     = 0
OMLSSU_RCV_SIPOCount     = 0
OMLSSU_RCV_SIBCount      = 0
OMLSSU_RCV_InvalidCount = 0

OMRemote_PO_Count        = 0
OMRemote_Congestion_Cnt = 0

OMtimeINSV (secs)        = 0
OMtimeNotINSV (secs)     = 9550
OMMSUBytesTransmitted    = 0
OMMSUBytesReceived       = 0

OMTransmitReqCount       = 33
OMPDU_notAcceptedCount   = 0
OMPDU_NACK_Count         = 0
OMunreasonableFSN_rcvd   = 0
OMunreasonableBSN_rcvd   = 0


OMT1_TMO_Count           = 0
OMT2_TMO_Count           = 0
OMT3_TMO_Count           = 0
OMT4_TMO_Count           = 0
OMT5_TMO_Count           = 0
OMT6_TMO_Count           = 0
OMT7_TMO_Count           = 0
OMT8_TMO_Count           = 0
OMTA_TMO_Count           = 0
OMTF_TMO_Count           = 0
OMTO_TMO_Count           = 0
OMTS_TMO_Count           = 477218
OMLostTimerCount         = 0

OMOMLostBackHaulMsgs     = 0

OMAERMCount              = 0
OMAERMFailCount          = 0
OMSUERMCount             = 0
OMSUERMFailCount         = 0
OMCongestionCount        = 0
OMCongestionBackhaulCnt = 0
```

Table 57 SS7 OM Information Fields

Field	Description
OMIACAlignAttemptCount OMIACAlignFailCount OMIACAlignCompleteCount	Counts for Initial Alignment Control (IAC) attempts.
OMMSU_TO_XMIT_Count	This count is related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. The number shown in OMMSU_TO_XMIT_Count is less than the PDU_pkts_recieve_count because OMMSU_TO_XMIT_Count shows the number of PDUs going out on the link, while the PDU_pkts_recieve_count includes PDUs that are internal to MTP2.
OMMSU_RCV_Count	Related to the results of the **show ss7 sm stats** command's packets_send_count.
OMLSSU_XMIT_Count OMLSSU_XMIT_SINCount OMLSSU_XMIT_SIECount OMLSSU_XMIT_SIOCount OMLSSU_XMIT_SIOSCount OMLSSU_XMIT_SIPOCount OMLSSU_XMIT_SIBCount	These counters represent the number of times that MTP 2 has posted the specific Link Status Signal Unit (LSSU) to MTP 1. They do *not* show the number of LSSUs actually sent over the link.
OMLSSU_RCV_Count OMLSSU_RCV_SINCount OMLSSU_RCV_SIECount OMLSSU_RCV_SIOCount OMLSSU_RCV_SIOSCount OMLSSU_RCV_SIPOCount OMLSSU_RCV_SIBCount OMLSSU_RCV_InvalidCount	These counters represent the number of LSSUs received by MTP 2 from MTP 1. Because of MTP 1 filtering, this is *not* the same as the actual LSSUs sent over the link.

Table 57 SS7 OM Information Fields (continued)

Field	Description
OMT1_TMO_Count OMT2_TMO_Count OMT3_TMO_Count OMT4_TMO_Count OMT5_TMO_Count OMT6_TMO_Count OMT7_TMO_Count OMT8_TMO_Count OMTA_TMO_Count OMTF_TMO_Count OMTO_TMO_Count OMTA_TMO_Count OMLostTimerCount	These fields show information about timers in use.
OMLostBackhaulMsgs	This count is related to the results of the **show ss7 sm stats** command's PDU_pkts_recieve_count statistic. The counter indicates how many messages received from the Media Gateway Controller have been lost because of a lack of resources in the Cisco 2600 series router. For example, if the Media Gateway Controller sends 100 MSUs and the Cisco 2600 series router only has 65 free buffers, 35 MSUs might be lost.

show ss7 mtp2 timer

To display durations of the SS7 MTP 2 state machine timers, use the **show ss7 mtp2 timer** command in privileged EXEC mode.

show ss7 mtp2 timer [*channel*]

Note The eight timers whose status is displayed using the **show ss7 mtp2 timer** command are set on the Media Gateway Controller using MML commands. The timers are then downloaded from the controller to the Cisco SLT.

Syntax Description

channel	Specifies a channel from 0 through 3.

Defaults

If you do not specify a channel, the command shows status information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

MTP 2 uses eight different timers on each link. Throughout the link state transitions, multiple timers are active. An in-service MTP 2 link requires timers that are constantly started, stopped, and restarted. Use this command to display the configured timer durations.

Note All MTP 2 configuration parameters are set at the Cisco SLT command line interface. The Media Gateway Controller parameter data files are no longer used to configure the Cisco SLT.

Examples

The following example shows how to display timer information for channel 0:

```
Router# show ss7 mtp2 timer 0
SS7 MTP2 Timers for channel 0 in milliseconds
Protocol version for channel 0 is Japan NTT Q.703 Version 1-1
    T1 aligned/ready = 15000
      T2 not aligned = 5000
          T3 aligned = 3000
T4 Emergency Proving = 3000
   T4 Normal Proving = 3000
      T5 sending SIB = 200
      T6 remote cong = 3000
 T7 excess ack delay = 2000
  T8 errored int mon = 0
TA SIE timer = 20
       TF FISU timer = 20
        TO SIO timer = 20
       TS SIOS timer = 20
```

show ss7 mtp2 variant

To display information about the SS7 MTP 2 protocol variant, use the **show ss7 mtp2 variant** command in privileged EXEC mode.

show ss7 mtp2 variant [*channel*]

Syntax Description

channel	Specifies a channel from 0 through 3.

Defaults

If you do not specify a channel, the command shows protocol information for channel 0.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Each country specifies its own variant of SS7, and the Cisco SLT supports several variants of the MTP 2 protocol. The selected variant can affect the MTP 2 statistics displayed by various commands. The Cisco SLT support the following variants:

- Telcordia Technologies (formerly Bellcore)
- ITU
- NTT (Japan)
- TTC (Japan Telecom)

Each channel can be configured to any one of the protocol variants. When you change from one variant to another, for example from Bellcore to NTT, the MTP 2 parameters default to those specified by NTT. You can then change the defaults as required.

Examples

The following example shows how to display protocol variant information for channel 1:

```
Router# show ss7 mtp2 variant 1
Protocol version for channel 1 is Bellcore GR-246-Core Issue 2, Dec 1997
```

show ss7 sm session

To display information about SS7 Session Manager session, use the **show ss7 sm session** command in privileged EXEC mode.

show ss7 sm session [*session*]

Syntax Description

session	Specifies a session, 0 or 1.

Defaults

If you do not specify a session, the command shows information for both sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no sessions are configured, the message "No Session is configured" appears.

Examples

The following example shows how to display session information for both sessions. Table 58 explains the fields.

```
Router# show ss7 sm session
Session[0]: Remote Host 255.255.251.254:8060, Local Host 255.255.255.254:8060
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32

Session[1]: Remote Host 255.255.251.255:8061, Local Host 255.255.255.254:8061
      retrans_t = 600
      cumack_t  = 300
      kp_t      = 2000
      m_retrans = 2
      m_cumack  = 3
      m_outseq  = 3
      m_rcvnum  = 32
```

Table 58 Session Manager Session Information

Field	Description
Remote Host, Local Host	Shows the IP address and port number for the session.
retrans_t	Shows the retransmission timer value.
cumack_t	Shows the cumulative acknowledgment timer value.
m_cumack	Shows the maximum number of segments that can be received before the RUDP sends an acknowledgment.
m_outseq	Shows the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
m_rcvnum	Shows the maximum number of segments that the remote end can send before receiving an acknowledgment

Related Commands

Command	Description
ss7 session retrans_t	Sets the retransmission timer.
ss7 session m_rcvnum	Sets the maximum number of segments that the remote end can send before receiving an acknowledgment.
ss7 session m_outseq	Sets the maximum number of out-of-sequence segments that can be received before the RUDP sends an extended acknowledgment.
ss7 session m_cumack	Sets the maximum number of segments that can be received before the RUDP sends an acknowledgment.
ss7 session cumack_t	Sets the cumulative acknowledgment timer.
ss7 session	Establishes a session.

show ss7 sm set

To display information about the SS7 failover timer, use the **show ss7 sm set** command in privileged EXEC mode.

show ss7 sm set

Syntax Description

There are no arguments or keywords.

Defaults

There is no default.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Examples

The following example shows how to display failover timer information; the failover timer is set to the default of 3 seconds:

```
Router# show ss7 sm set
Session Manager Set
      failover timer = 3 seconds
```

Related Commands

Command	Description
ss7 set failover timer	Specifies the amount of time that the Session Manager waits for the session to recover before declaring the session inactive.
ss7 session	Establishes a session.

show ss7 sm stats

To display SS7 Session Manager session statistics, use the **show ss7 sm stats** command in privileged EXEC mode.

show ss7 sm stats

Syntax Description

There are no arguments or keywords for this command.

Defaults

The command shows information for both sessions.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR	This command was introduced.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

If no sessions are configured, the message "No Session is configured" appears.

Examples

The following example shows how to display SS7 Session Manager statistics. The fields are self-explanatory and show information about the session state, protocol data units (PDUs) packets sent and received, and SS7 Reliable User Datagram Protocol (RUDP) performance:

```
Router# show ss7 sm stats

-------------------- Session Manager  --------------------

Session Manager state             = SESSION SET STATE-ACTIVE
Session Manager Up count          = 1
Session Manager Down count        = 0
   lost control packet count      = 0
              lost PDU count      = 0
 failover timer expire count      = 0
 invalid_connection_id_count      = 0

Session[0] statistics  SM SESSION STATE-STANDBY:
Session Down count               = 0
   Open Retry count              = 0

   Total Pkts receive count      = 1
   Active Pkts receive count     = 0
   Standby Pkts receive count    = 1
   PDU Pkts receive count        = 0
   Unknown Pkts receive count    = 0
```

```
   Pkts send count               = 0
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0

   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0

Session[1] statistics  SM SESSION STATE-ACTIVE:
Session Down count               = 0
   Open Retry count              = 0

   Total Pkts receive count      = 2440
   Active Pkts receive count     = 1
   Standby Pkts receive count    = 0
   PDU Pkts receive count        = 2439
   Unknown Pkts receive count    = 0

   Pkts send count               = 2905
   Pkts requeue count            = 0
    -Pkts window full count      = 0
    -Pkts resource unavail count = 0
    -Pkts enqueue fail count     = 0
   PDUs dropped (Large)          = 0
   PDUs dropped (Empty)          = 0

   RUDP Not Ready Errs           = 0
   RUDP Connection Not Open      = 0
   RUDP Invalid Conn Handle      = 0
   RUDP Unknown Errors           = 0
   RUDP Unknown Signal           = 0
   NonActive Receive count       = 0
```

Related Commands

Command	Description
clear ss7 sm-stats	Clears the counters that track Session Manager statistics for the **show ss7 sm stats** command.
ss7 session	Establishes a session.

show translation-rule

To display the contents of the rules that have been configured for a specific translation name, use the **show translation-rule** command in privileged EXEC mode.

show translation-rule [*name-tag*]

Syntax Description

name-tag	(Optional) The tag number by which the rule set will be referenced. This is an arbitrarily chosen number. The range is from 1 through 2,147,483,647.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)XR1	This command was introduced for Voice over IP on the Cisco AS5300 universal access server.
12.0(7)XK	This command was first supported for the following voice technologies on the following platforms: • Voice over IP (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) • Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) • Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)
12.1(1)T	This command was first supported on the T train for the following voice technology on the following platforms: • Voice over IP (1750, Cisco 2600 series, Cisco 3600 series, Cisco AS5300 universal access server, Cisco 7200 series, and Cisco 7500 series)
12.1(2)T	This command was first supported on the T train for the following voice technologies on the following platforms: • Voice over IP (Cisco MC3810 multiservice concentrator) • Voice over Frame Relay (Cisco 2600 series, Cisco 3600 series, Cisco MC3810 multiservice concentrator) • Voice over ATM (Cisco 3600 series, Cisco MC3810 multiservice concentrator)

Usage Guidelines

This command gives detailed information about the configured rules under this rule name. If the name tag is not entered, a complete display of all the configured rules will be shown.

Examples

The following example shows output for the **show translation-rule** command:

```
Router# show translation-rule

Translation rule address:0x61AB94F8
Tag name:21
Translation rule in_used 1
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:555.%
        Sub  pattern:1408555
        Match  type:subscriber
        Sub type:international
**** Xrule rule table *******
        Rule :2
        in_used state:1
        Match pattern:8.%
        Sub  pattern:1408555
        Match  type:abbreviated
        Sub type:international
Translation rule address:0x61C2E6D4
Tag name:345
Translation rule in_used 1
**** Xrule rule table *******
        Rule :1
        in_used state:1
        Match pattern:.%555.%
        Sub  pattern:7
        Match  type:ANY
        Sub type:abbreviated
```

Table 59 describes the significant fields shown in the display.

Table 59 show translation-rule Field Descriptions

Translation rule address	The translation rule address in hex.
Tag name	The translation rule tag name.
Translation rule in_used	The translation rule in which the tag is used.
**** Xrule rule table *******	Specifies the beginning of the display for a specific rule.
Rule:x	The number of the rule.
in_used state:	The input-searched-pattern.
Match pattern:	The match pattern of the rule.
Sub pattern:	The substituted pattern.
Match type:	The match type.
Sub type:	The substituted pattern match type.

Related Commands

Command	Description
numbering-type	Specifies number type for the VoIP or POTS dial peer.
rule	Applies a translation rule to a calling party number or a called party number for both incoming and outgoing calls.
test translation-rule	Tests the execution of the translation rules on a specific name-tag.

Command	Description
translate	Applies a translation rule to a calling party number or a called party number for incoming calls.
translate-outgoing	Applies a translation rule to a calling party number or a called party number for outgoing calls.
translation-rule	Creates a translation name and enters translation-rule configuration mode.
voip-incoming translation-rule	Captures calls that originate from H.323-compatible clients.

show vfc

To see the entries in the host-name-and-address cache, use the **show vfc** command in privileged EXEC mode.

show vfc *slot-number* [**technology**]

Syntax Description

slot-number	VFC slot number.
technology	(Optional) Displays the technology type of the VFC.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.
12.0(2)XH	The **technology** keyword was added.

Examples

The following example shows that the card in slot 1 is a C549 DSPM:

```
Router# show vfc 1 technology

Technology in VFC slot 1 is C549
```

Related Commands

Command	Description
voice-card	Configures a voice card and enters voice-card configuration mode.

show vfc cap-list

To show the current list of files on the capability list for this voice feature card (VFC), use the **show vfc cap-list** command in user EXEC mode.

show vfc *slot* **cap-list**

Syntax Description

slot	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.

Defaults

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

To identify the specific VFC, enter the number of the slot on the chassis where the VFC resides using the *slot* argument.

Examples

The following is sample output from the **show vfc cap-list** command:

```
Router# show vfc 1 cap-list

Capability List for VFC in slot 1:
1. fax-vfc-l.0.1.bin
2. bas-vfc-l.0.1.bin
3. cdc-g729-l.0.1.bin
4. cdc-g711-l.0.1.bin
5. cdc-g726-l.0.1.bin
6. cdc-g728-l.0.1.bin
7. cdc-gsmfr-l.0.1.bin
```

The first line in this output is a general description, stating that this is the capability list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one currently installed in-service file.

Related Commands

Command	Description
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc default-file

To show the default files included in the default file list for a voice feature card (VFC), use the **show vfc default-file** command in user EXEC mode.

show vfc *slot* **default-file**

Syntax Description

slot	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.

Defaults

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **show vfc default-file** user EXEC command to display a list of all default files for a particular voice feature card. To identify the specific VFC, enter the number of the slot on the chassis where the VFC resides using the *slot* argument.

Examples

The following is sample output from the **show vfc default-file** command:

```
Router# show vfc 1 default-file

Default List for VFC in slot 1:
1. btl-vfc-l.0.13.0.bin
2. cor-vfc-l.0.1.bin
3. bas-vfc-l.0.1.bin
4. cdc-g729-l.0.1.bin
5. fax-vfc-l.0.1.bin
6. jbc-vfc-l.0.13.0.bin
```

The first line in this output is a general description, stating that this is the default list for the VFC residing in slot 1. Below this is a numbered list, each line of which identifies one default file.

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc directory

To show the list of all files residing on a voice feature card (VFC), use the **show vfc directory** command in user EXEC mode.

show vfc *slot* **directory**

Syntax Description

slot	Identifies the slot where the VFC is installed. Valid entries are from 0 to 2.

Defaults

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **show vfc directory** user EXEC command to display a list of all of the files currently stored in Flash memory for a particular VFC. To identify the specific VFC, enter the number of the slot on the chassis where the VFC resides using the *slot* argument.

Examples

The following is sample output from the **show vfc directory** command:

```
Router# show vfc 1 directory

Files in slot 1  VFC flash:
     File Name                         Size (Bytes)
1 .  vcw-vfc-mz.gsm.VCW                292628
2 .  btl-vfc-l.0.13.0.bin              4174
3 .  cor-vfc-l.0.1.bin                 54560
4 .  jbc-vfc-l.0.13.0.bin              16760
5 .  fax-vfc-l.0.1.bin                 64290
6 .  bas-vfc-l.0.1.bin                 54452
7 .  cdc-g711-l.0.1.bin                190
8 .  cdc-g729-l.0.1.bin                21002
9 .  cdc-g726-l.0.1.bin                190
10.  cdc-g728-l.0.1.bin                22270
11.  cdc-gsmfr-l.0.1.bin               190
```

Table 60 describes the significant fields shown in the display.

Table 60 show vfc directory Field Descriptions

Field	Description
File Name	Name of the file stored in Flash memory.
Size (Bytes)	Size of the file in bytes.

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc version	Displays the version of the software residing on this VFC.

show vfc version

To show the version of the software residing on a voice feature card (VFC), use the **show vfc version** command in user EXEC mode.

show vfc *slot* **version** {**dspware** | **vcware**}

Syntax Description

slot	Identifies the slot where the VFC is installed. Valid values are 0, 1, and 2.
dspware	Defines which DSPWare software to display.
vcware	Defines which VCWare software to display.

Defaults

No default behavior or values.

Command Modes

User EXEC

Command History

Release	Modification
11.3 NA	This command was introduced on the Cisco AS5300 universal access server.

Usage Guidelines

Use the **show vfc version** user EXEC command to display the version of the software (running on either DSP or VFC) currently installed in Flash memory on the VFC.

Examples

The following is sample output from the **show vfc version** command:

```
Router# show vfc 0 version dspware

Version of Dspware in VFC slot 0 is 0.10
```

The output from this command is a simple declarative sentence stating the version number for the selected type of software (in this example, DSPWare) for the VFC residing in the selected slot number (in this example, slot 0).

Related Commands

Command	Description
show vfc cap-list	Displays the current list of files on the capability list for this VFC.
show vfc default-file	Displays the default files included in the default file list for this VFC.
show vfc directory	Displays the list of all files residing on this VFC.

show video call summary

To display summary information about video calls and the current status of the Video Call Manager (ViCM), use the **show video call summary** command in privileged EXEC mode.

show video call summary

Syntax Description

There are no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)XK	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)T	The command introduced in Cisco IOS Release 12.0(5)XK was integrated into Cisco IOS Release 12.0(7)T.

Usage Guidelines

Use this command to look quickly at the status of current calls. In Cisco IOS Releases 12.0(5)XK and 12.0(7)T, there can be only one video call in progress.

Examples

On a Cisco MC3810 multiservice concentrator, the following example displays information about the ViCM when no call is in progress on the serial interface that connects to the local video codec:

```
Router# show video call summary

Serial0:ViCM = Idle, Codec Ready
```

When a call is starting, the output looks like this:

```
Router# show video call summary

Serial0:ViCM = Call Connected
```

When a call is disconnecting, the output looks like this:

```
Router# show video call summary

Serial0:ViCM = Idle
```

Related Commands

Command	Description
show call history video record	Displays information about video calls.

show voice busyout

To display information about the voice busyout state, use the **show voice busyout** command in privileged EXEC mode.

show voice busyout

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

The **show voice busyout** command lists the following information:

- Interfaces that are being monitored for busyout events
- Voice ports currently in the busyout state and the reasons

Examples

The following example displays the busyout information:

```
Router# show voice busyout

If following network interfaces are down, voice port will be put into busyout state
ATM0
Serial0
The following voice ports are in busyout state

1/1     is forced into busyout state
1/2     is in busyout state caused by network interfaces
1/3     is in busyout state caused by ATM0
1/4     is in busyout state caused by network interfaces
1/5     is in busyout state caused by Serial0
```

Related Commands

Command	Description
busyout forced	Forces a voice port into the busyout state.
busyout monitor	Places a voice port in the busyout monitor state.
busyout seize	Changes the busyout seize procedure from a voice port.
voice-port busyout	Places all voice ports associated with a serial or ATM interface in a busyout state.

show voice call

To show the call status for voice ports on the Cisco router or concentrator, use the **show voice call** EXEC command.

Cisco 2600 and 3600 series with Analog Voice Ports

show voice call [*slot*/*subunit*/*port* | **summary**]

Cisco 2600 and 3600 Series with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)

show voice call [*slot*/*port***:***ds0-group* | **summary**]

Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

show voice call [*slot*/*port* | **summary**]

Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

show voice call [*slot***:***ds0-group* | **summary**]

Syntax Description

For the Cisco 2600 and 3600 Series with Analog Voice Ports:

slot/*subunit*/*port*	(Optional) Displays information for the analog voice port you specify with the *slot/subunit/port* designation. • *slot* specifies a router slot in which a voice network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit* specifies a voice interface card (VIC) where the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) • *port* specifies an analog voice port number. Valid entries are 0 and 1.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco 2600 and 3600 Series with Digital Voice Ports:

slot/*port***:***ds0-group*	(Optional) Displays information for the digital voice port you specify with the *slot/port:ds0-group* designation. • *slot* specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *port* specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.) • *ds0-group* specifies a T1 or E1 logical port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports:

slot/*port*	(Optional) Displays information for the analog voice port you specify with the *slot*/*port* designation. • *slot* is the physical slot in which the analog voice module (AVM) is installed. The *slot* is always 1 for analog voice ports in the Cisco MC3810 multiservice concentrator. • *port* specifies an analog voice port number. Valid entries are from 1 to 6.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports:

*slot***:***ds0-group*	(Optional) Displays information for the digital voice port you specify with the *slot*:*ds0-group* designation. • *slot* specifies the module (and controller). Valid entries are 0 for the MFT (controller 0) and 1 for the DVM (controller 1). • *ds0-group* specifies a T1 or E1 logical voice port number. Valid entries are 0 to 23 for T1 and 0 to 30 for E1.
summary	(Optional) Displays a summary of all voice ports.

Command Modes

EXEC

Command History

Release	Modification
11.3(1)MA	This command was introduced for the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

The **show voice call** command applies to Voice over Frame Relay, Voice over ATM, and Voice over IP.

This command shows call-processing and protocol state-machine information for a voice port, if it is available. It also shows information on the DSP channel associated with the voice port, if it is available. All real-time information in the DSP channel, such as jitter and buffer overrun for example, is queried to the DSP channel, and asynchronous responses are returned to the host side.

If no call is active on a voice port, the **show voice call summary** command displays only the VPM (shutdown) state. If a call is active on a voice port, the VTSPS state is shown. For an on-net call or a local call without local-bypass (not cross-connected), the CODEC and VAD fields are displayed. For an off-net call or a local call with local-bypass, the CODEC and VAD fields are not displayed.

CODEC and VAD are not displayed by the **show voice call** command because this information is in the summary display.

The **show voice call** command provides the status at these levels of the call handling module:

- Tandem switch
- End-to-end call manager
- Call processing state machine
- Protocol state machine

Examples

The following is a sample display from the **show voice call summary** command for voice ports on a Cisco MC3810 multiservice concentrator, showing two local calls connected without local bypass:

```
PORT    CODEC    VAD VTSP STATE            VPM STATE
======= ======== === ==================== ========================
0:17.18                                    *shutdown*
0:18.19 g729ar8   n  S_CONNECT            FXOLS_OFFHOOK
0:19.20                                   FXOLS_ONHOOK
0:20.21                                   FXOLS_ONHOOK
0:21.22                                   FXOLS_ONHOOK
0:22.23                                   FXOLS_ONHOOK
0:23.24                                   EM_ONHOOK
1/1                                       FXSLS_ONHOOK
1/2                                       FXSLS_ONHOOK
1/3                                       EM_ONHOOK
1/4                                       EM_ONHOOK
1/5                                       FXOLS_ONHOOK
1/6     g729ar8   n  S_CONNECT            FXOLS_CONNECT
```

The following is a sample display from the **show voice call summary** command for voice ports on a Cisco MC3810 multiservice concentrator, showing two local calls connected with local bypass:

```
PORT    CODEC    VAD VTSP STATE            VPM STATE
======= ======== === ==================== ========================
0:17.18                                    *shutdown*
0:18.19              S_CONNECT            FXOLS_OFFHOOK
0:19.20                                   FXOLS_ONHOOK
0:20.21                                   FXOLS_ONHOOK
0:21.22                                   FXOLS_ONHOOK
0:22.23                                   FXOLS_ONHOOK
0:23.24                                   EM_ONHOOK
1/1                                       FXSLS_ONHOOK
1/2                                       FXSLS_ONHOOK
1/3                                       EM_ONHOOK
1/4                                       EM_ONHOOK
1/5                                       FXOLS_ONHOOK
1/6                  S_CONNECT            FXOLS_CONNECT
```

The following is a sample display from the **show voice call** command for analog voice ports on a Cisco MC3810 multiservice concentrator:

```
1/1 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/2 vpm level 1 state = FXSLS_ONHOOK
vpm level 0 state = S_UP
1/3 is shutdown
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
1/5 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP
1/6 vpm level 1 state = EM_ONHOOK
vpm level 0 state = S_UP
```

```
sys252#show voice call 1/4
1/4 vtsp level 0 state = S_CONNECT
vpm level 1 state = S_TRUNKED
vpm level 0 state = S_UP
router#***DSP VOICE VP_DELAY STATISTICS***
Clk Offset(ms): 1445779863, Rx Delay Est(ms): 95
Rx Delay Lo Water Mark(ms): 95, Rx Delay Hi Water Mark(ms): 125
***DSP VOICE VP_ERROR STATISTICS***
Predict Conceal(ms): 10, Interpolate Conceal(ms): 0
Silence Conceal(ms): 0, Retroact Mem Update(ms): 0
Buf Overflow Discard(ms): 20, Talkspurt Endpoint Detect Err: 0
***DSP VOICE RX STATISTICS***
Rx Vox/Fax Pkts: 537, Rx Signal Pkts: 0, Rx Comfort Pkts: 0
Rx Dur(ms): 50304730, Rx Vox Dur(ms): 16090, Rx Fax Dur(ms): 0
Rx Non-seq Pkts: 0, Rx Bad Hdr Pkts: 0
Rx Early Pkts: 0, Rx Late Pkts: 0
***DSP VOICE TX STATISTICS***
Tx Vox/Fax Pkts: 567, Tx Sig Pkts: 0, Tx Comfort Pkts: 0
Tx Dur(ms): 50304730, Tx Vox Dur(ms): 17010, Tx Fax Dur(ms): 0
***DSP VOICE ERROR STATISTICS***
Rx Pkt Drops(Invalid Header): 0, Tx Pkt Drops(HPI SAM Overflow): 0
***DSP LEVELS***
TDM Bus Levels(dBm0): Rx -70.3 from PBX/Phone, Tx -68.0 to PBX/Phone
TDM ACOM Levels(dBm0): +2.0, TDM ERL Level(dBm0): +5.6
TDM Bgd Levels(dBm0): -71.4, with activity being voice
```

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.

show voice dsp

To show the current status of all digital signal processor (DSP) voice channels, use the **show voice dsp** command in privileged EXEC mode.

show voice dsp

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.3(1)MA	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(7)XK	This command was first supported on the Cisco 2600 and 3600 series routers, and the display format was modified.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

Use this command when abnormal behavior in the DSP voice channels occurs.

Examples

The following is sample output from the **show voice dsp** command on a Cisco MC3810 multiservice concentrator:

```
Router# show voice dsp

DSP# 0, channel# 0 G729A BUSY
DSP# 0, channel# 1 G729A BUSY
DSP# 1, channel# 2 FAX IDLE
DSP# 1, channel# 3 FAX IDLE
DSP# 2, channel# 4 NONE BAD
DSP# 2, channel# 5 NONE BAD
DSP# 3, channel# 6 NONE BAD
DSP# 3, channel# 7 NONE BAD
DSP# 4, channel# 8 NONE BAD
DSP# 4, channel# 9 NONE BAD
DSP# 5, channel# 10 NONE BAD
DSP# 5, channel# 11 NONE BAD
```

Table 61 describes the significant fields shown in the display.

Table 61 show voice dsp Field Descriptions

Field	Description
DSP	Number of the DSP.
Channel	Number of the channel and its status.

The following is sample output from the **show voice dsp** command on a Cisco 1750 router:

```
Router# show voice dsp

DSP#0: state IN SERVICE, 2 channels allocated
channel#0: voice port 1/0, codec G711 ulaw, state UP
channel#1: voice port 1/1, codec G711 ulaw, state UP
DSP#1: state IN SERVICE, 2 channels allocated
channel#0: voice port 2/0, codec G711 ulaw, state UP
channel#1: voice port 2/1, codec G711 ulaw, state UP
DSP#2: state RESET, 0 channels allocated
```

Table 62 describes the significant fields shown in the display.

Table 62 show voice dsp Field Descriptions

Field	Description
DSP	Number of the DSP.
Channel	Number of the channel and its status.

Related Commands

Command	Description
clear counters	Clears all the current interface counters from the interface.
show dial-peer voice	Displays configuration information for dial peers.
show voice call	Displays the call status for all voice ports.
show voice port	Displays configuration information about a specific voice port.

show voice permanent-call

To display information about the permanent calls on a voice interface, use the **show voice permanent-call** command in user EXEC or privileged EXEC mode.

show voice permanent-call [*voice-port*] [**summary**]

Syntax Description

voice-port	(Optional) Slot number or slot/port number of the voice interface for which you wish to display permanent call information.
summary	(Optional) Displays summary information about VoFR and VoATM ports used for permanent connections.

Defaults

No default behavior or values.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator.
12.0(4)T	The command introduced in Cisco IOS Release 12.0(3)XG was integrated into Cisco IOS Release 12.0(4)T.

Usage Guidelines

This command is available only on the Cisco MC3810 multiservice concentrator.

When no parameters are specified with this command, the output displays information for all ports containing permanent calls. When a specific interface is specified, information is displayed about the permanent calls for that interface only.

Examples

The following is sample output for the **show voice permanent-call** command:

```
Router# show voice permanent-call 1/1

1/1 state=connect coding=G729A payload size=30 vad=off
ec=8 (ms), cng=off fax=on digit_relay=on Seq num = off, VOFR Serial0,dlci = 550,cid = 6
TX INFO :slow-mode seq#= 25, sig pkt cnt= 19646, last-ABCD=1101
hardware-state ACTIVE signal type is CEPT/MELCAS
voice-gate CLOSED,network-path OPEN MASTER
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
 1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
RX INFO :slow-mode, sig pkt cnt= 19648, under-run = 0, over-run = 0
missing = 0, out of seq = 0, very late = 0
playout depth = 0 (ms), refill count = 1
 prev-seq#= 25, last-ABCD=1101, slave standby timeout 25000 (ms)
max inter-arrival time 0 (ms), current timer 384 (ms)
```

```
max timeout timer 5016 (ms), restart timeout is 0 (ms)
signaling packet fast-mode inter-arrival times (ms)
16 24 16 24 16 24 16 24 16 24 16 24 16 24 16 24
16 24 16 24 16 24 16 24 0 0 0 0 0 0 0 0

signaling playout history
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
1101 1101 1101 1101 1101 1101 1101 1101 1101 1101
```

The following is sample output for the **show voice permanent-call summary** command:

```
Router# show voice permanent-call summary

1/1 state= connect, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 880,cid = 6
1/2 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 102
1/3 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 103
1/4 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 104
1/5 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 105
1/6 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 106
1/7 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 107
1/8 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 108
1/9 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 109
1/10 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 110
1/11 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 111
1/12 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 112
1/13 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 113
1/14 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 114
1/15 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 115
1/17 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 117
1/18 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 118
1/19 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 119
1/20 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 120
1/21 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 121
1/22 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 122
1/23 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 123
1/24 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 124
1/25 state= frf11, coding=G729A, payload size=30, vad=off, ec=64, cng=off, fax=on
  digit_relay=off, VOFR Serial0:1,dlci = 990,cid = 125
```

Table 63 describes the fields shown in these displays.

Table 63 show voice permanent-call Field Descriptions

Field	Description
state	Current status of the call on this voice port.
coding	Codec type used for this call.
payload size	Size in bytes of the voice payload.
vad	Indicates whether voice activity detection is turned on or off.
ec	Echo canceler length, in milliseconds.
cng	Indicates whether or not comfort noise generation is used.
fax	Indicates if fax-relay is enabled.
digit_relay	Indicates if FRF.11 Annex A DTMF digit-relay is enabled.
Seq num	Indicates whether sequence numbers are turned on or off.
VOFR	Interface used for this call.
dlci	DLCI for this call.
cid	DLCI subchannel for this call.
TX INFO:slow-mode	Indicates that FRF.11 Annex B packets are being sent at the slow rate defined by the signal timing keepalive period.
TX INFO:seq#	Sequence number of the last packet sent.
TX INFO:sig pkt cnt	Number of signaling packets sent by this dial peer.
TX INFO:last-ABCD	Last ABCD signaling state sent by this dial peer to the network.
hardware-state	Indicates the on-hook/off-hook state of the call when the signaling protocol in use is a supported protocol. Not valid when the signal type is “transparent.”
signal type	Indicates the type of call-control signaling used by this dial peer.
voice-gate	Indicates whether voice packets are being sent (OPEN) or not sent (CLOSED).
network-path	Indicates if any type of packet is being sent (OPEN) or not sent (CLOSED) to the network. This field will indicate CLOSED only if the port is configured as a slave using the **connection trunk answer-mode** command.
RX INFO:slow-mode	Indicates that FRF.11 Annex B packets are being received at the slow rate. Successive packets have the same sequence number.
RX INFO:sig pkt cnt	Number of slow-mode signaling packets received by this dial peer.
RX INFO:under-run	Valid for fast-mode only. Counts the number of times the signaling playout buffer became empty during FRF.11 Annex B fast-mode. In this mode, signaling packets are expected to be received every 20 milliseconds.
RX INFO:over-run	Valid for fast-mode only. Counts the number of times the signaling playout buffer became full during FRF.11 Annex B fast-mode. In this mode, signaling packets are expected to be received every 20 milliseconds.

Table 63 show voice permanent-call Field Descriptions (continued)

Field	Description
RX INFO:missing	Indicates the number of FRF.11 Annex B packets that were counted as missing based on checking Annex B sequence numbers.
RX INFO:out of seq	Number of FRF.11 Annex B packets that were counted as received in the wrong order based on checking Annex B sequence numbers.
RX INFO:very late	Number of FRF.11 Annex B packets that were received with a sequence number significantly different from the expected sequence number.
RX INFO:playout depth	Valid for fast-mode only. Shows the current FRF.11 Annex B signaling buffer playout depth in milliseconds.
RX INFO:refill count	Indicates the number of times the FRF.11 Annex B signaling playout buffer was refilled as a result of a slow-mode to fast-mode transition.
RX INFO:prev-seq#	Sequence number of the last FRF.11 Annex B signaling packet received.
RX INFO:last-ABCD	Last ABCD signaling bit pattern sent to the attached PBX (telephone network side). In the out-of-service condition, this will show the OOS pattern being sent to the PBX.
RX INFO:slave standby timeout	Value configured using the **signal timing oos standby** command for the applicable voice class permanent entry.
max inter-arrival time	Maximum interval between the arrival of fast-mode FRF.11 Annex B packets since the last time this parameter was displayed.
current timer	Time, in milliseconds, since the last signaling packet was received.
max timeout timer	Maximum value of the “current timer” parameter since the last time it was displayed.
restart timeout	Connection restart timeout value.
signaling packet fast-mode inter-arrival time	Shows the last several values of the fast-mode FRF.11 Annex B signaling packet inter-arrival time.
signaling playout history	Shows recent ABCD signaling bits received from the data network.

Related Commands

Command	Description
show frame-relay fragment	Displays Frame Relay fragmentation details.
show frame-relay pvc	Displays statistics about PVCs for Frame Relay interfaces.
show frame-relay vofr	Displays details about FRF.11 subchannels being used on Voice over Frame Relay DLCIs.

show voice port

To display configuration information about a specific voice port, use the **show voice port** command in EXEC command.

Cisco 1750 Router

show voice port *slot-number*/*port*

Cisco 2600 and 3600 Series Router with Analog Voice Ports

show voice port [*slot*/*subunit*/*port* | **summary**]

2600 and 3600 Series Router with Digital Voice Ports (with T1 Packet Voice Trunk Network Modules)

show voice port [*slot*/*port:ds0-group* | **summary**]

Cisco MC3810 Multiservice Concentrator with Analog Voice Ports

show voice port [*slot*/*port* | **summary**]

Cisco MC3810 Multiservice Concentrator with Digital Voice Ports

show voice port [*slot*:*ds0-group* | **summary**]

Cisco AS5300 Universal Access Server

show voice port *controller number*:**D**

Cisco AS5800 Universal Access Server

show voice port {*shelf/slot/port*:**D**} | {*shelf*/*slot*/*parent*:*port*:**D**}

Cisco 7200 Series Router

show voice port {*slot/port:ds0-group-no*} | {*slot-number*/*subunit-number*/*port*}

Syntax Description

For the Cisco 1750 Router:

slot-number	Slot number in the router where the voice interface card (VIC) is installed. Valid entries are from 0 to 2, depending on the slot where it has been installed.
port	Indicates the voice port. Valid entries are 0 or 1.

For the Cisco 2600 and 3600 Series Router with Analog Voice Ports:

slot/*subunit*/*port*	(Optional) Displays information for the analog voice port you specify with the *slot/subunit/port* designation. • *slot* specifies a router slot in which a voice network module (VNM) is installed. Valid entries are router slot numbers for the particular platform. • *subunit* specifies a voice interface card (VIC) where the voice port is located. Valid entries are 0 and 1. (The VIC fits into the voice network module.) • *port* specifies an analog voice port number. Valid entries are 0 and 1.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco 2600 and 3600 Series Router with Digital Voice Ports:

slot/*port:ds0-group*	(Optional) Displays information for the digital voice port you specify with the *slot/port:ds0-group* designation. • *slot* specifies a router slot in which the packet voice trunk network module (NM) is installed. Valid entries are router slot numbers for the particular platform. • *port* specifies a T1 or E1 physical port in the voice WAN interface card (VWIC). Valid entries are 0 and 1. (One VWIC fits in an NM.) • *ds0-group* specifies a T1 or E1 logical port number. Valid entries are from 0 to 23 for T1 and from 0 to 30 for E1.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco MC3810 Multiservice Concentrator with Analog Voice Ports:

slot/*port*	(Optional) Displays information for the analog voice port you specify with the *slot/port* designation. • *slot* is the physical slot in which the analog voice module (AVM) is installed. The *slot* is always 1 for analog voice ports in the Cisco MC3810 multiservice concentrator. • *port* specifies an analog voice port number. Valid entries are from 1 to 6.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco MC3810 Multiservice Concentrator with Digital Voice Ports:

slot:ds0-group	(Optional) Displays information for the digital voice port you specify with the *slot:ds0-group* designation. • *slot* specifies the module (and controller). Valid entries are 0 for the MFT (controller 0) and 1 for the DVM (controller 1). • *ds0-group* specifies a T1 or E1 logical voice port number. Valid entries are from 0 to 23 for T1 and from 0 to 30 for E1.
summary	(Optional) Displays a summary of all voice ports.

For the Cisco AS5300 Access Server :

controller number	Specifies the T1 or E1 controller.
:D	Indicates the D channel associated with ISDN PRI.

For the Cisco AS5800 Universal Access Server:

shelf/slot/port	Specifies the T1 or E1 controller on the T1 card. Valid entries for the *shelf* argument are from 0 to 9999. Valid entries for the *slot* argument are from 0 to 11. Valid entries for the *port* argument are from 0 to 11.
shelf/*slot*/*parent***:***port*	Specifies the T1 controller on the T3 card. Valid entries for the *shelf* argument are from 0 to 9999. Valid entries for the *slot* argument are from 0 to 11. Valid entries for the *port* argument is 1 to 28. The value for the *parent* argument is always 0.
:D	Indicates the D channel associated with ISDN PRI.

For the Cisco 7200 Series Router:

slot	The router location where the voice port adapter is installed. Valid entries are from 0 to 3.
port	Indicates the voice interface card location. Valid entries are 0 and 1.
dso-group-no	Indicates the defines DS0 group number. Each defined DS0 group number is represented on a separate voice port. This allows you to define individual DS0s on the digital T1/E1 card.
slot-number	Indicates the slot number in the Cisco router where the voice interface card is installed. Valid entries are from 0 to 3, depending on the slot where it has been installed.
subunit-number	Indicates the subunit on the voice interface card where the voice port is located. Valid entries are 0 and 1.
port	Indicates the voice port number. Valid entries are 0 and 1.

Defaults

No default behavior or values.

Command Modes

EXEC

Command History

Release	Modification
11.3(1) T	This command was introduced on the Cisco 3600 series router.
11.3(1)MA	Port-specific values for the Cisco MC3810 multiservice concentrator were added.
12.0(3)T	Port-specific values for the Cisco MC3810 multiservice concentrator were added.
12.0(5)XK	The *ds0-group* argument was added for the Cisco 2600 and Cisco 3600 series routers.
12.0(5)XE	Additional syntax was created for digital voice to allow specification of the DS0 group. This command applies to VoIP on the Cisco 7200 series.
12.0(7)T	The additions from Cisco IOS Release 12.0(5)XE were integrated into Cisco IOS Release 12.0(7)T.
12.0(7)XK	The **summary** keyword was added for the Cisco 2600 and 3600 series routers. The *ds0-group* argument was added for the Cisco MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into the 12.1(2)T release.

Usage Guidelines

Use the **show voice port** EXEC command to display configuration and voice-interface-card-specific information about a specific port.

This command applies to Voice over IP, Voice over Frame Relay, and Voice over ATM.

The **ds0-group** command automatically creates a logical voice port that is numbered as follows on Cisco 7200 series routers and the Cisco 2600 and Cisco 3600 series routers: *slot*/*port*:*ds0-group-no*. Although only one voice port is created for each group, applicable calls are routed to any channel in the group.

Examples

The following is sample output from the **show voice port summary** command for all voice ports on a Cisco MC3810 multiservice concentrator with an analog voice module (AVM):

```
IN   OUT   ECHO
PORT SIG-TYPE     ADMIN OPER IN-STATUS OUT-STATUS GAIN ATTN CANCEL
1/1  fxs-ls       up    up   on-hook    idle        0    0    y
1/2  fxs-ls       up    up   on-hook    idle        0    0    y
1/3  e&m-wnk      up    up   idle       idle        0    0    y
1/4  e&m-wnk      up    up   idle       idle        0    0    y
1/5  fxo-ls       up    up   idle       on-hook     0    0    y
1/6  fxo-ls       up    up   idle       on-hook     0    0    y
```

The following is sample output from the **show voice port summary** command on a Cisco MC3810 multiservice concentrator with a digital voice module (DVM):

```
                                  IN       OUT
PORT   CH SIG-TYPE   ADMIN OPER STATUS   STATUS   EC
====== == ========== ===== ==== ======== ======== ==
0:17   18 fxo-ls     down  down idle     on-hook  y
0:18   19 fxo-ls     up    dorm idle     on-hook  y
0:19   20 fxo-ls     up    dorm idle     on-hook  y
0:20   21 fxo-ls     up    dorm idle     on-hook  y
```

```
0:21   22 fxo-ls     up    dorm idle     on-hook  y
0:22   23 fxo-ls     up    dorm idle     on-hook  y
0:23   24 e&m-imd    up    dorm idle     idle     y
1/1    -- fxs-ls     up    dorm on-hook  idle     y
1/2    -- fxs-ls     up    dorm on-hook  idle     y
1/3    -- e&m-imd    up    dorm idle     idle     y
1/4    -- e&m-imd    up    dorm idle     idle     y
1/5    -- fxo-ls     up    dorm idle     on-hook  y
1/6    -- fxo-ls     up    dorm idle     on-hook  y
Elements :
sys/voip/ccvpm                vpm_htsp.c (107)
sys/voip/ccvtsp               vtsp_core.c (167)
sys/voip/cli                  voiceport_action.c (58)

receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is E&M
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

The following is sample output from the **show voice port** command for an E&M analog voice port on a Cisco 3600:

```
E&M Slot is 1, Sub-unit is 0, Port is 0
 Type of VoicePort is E&M
 Operation State is unknown
 Administrative State is unknown
 The Interface Down Failure Cause is 0
 Alias is NULL
 Noise Regeneration is disabled
 Non Linear Processing is disabled
 Music On Hold Threshold is Set to 0 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is disabled
 Echo Cancel Coverage is set to 16ms
 Connection Mode is Normal
 Connection Number is
 Initial Time Out is set to 0 s
 Interdigit Time Out is set to 0 s
 Analog Info Follows:
 Region Tone is set for northamerica
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0

 Voice card specific Info Follows:
 Signal Type is wink-start
 Operation Type is 2-wire
 Impedance is set to 600r Ohm
 E&M Type is unknown
```

```
 Dial Type is dtmf
 In Seizure is inactive
 Out Seizure is inactive
 Digit Duration Timing is set to 0 ms
 InterDigit Duration Timing is set to 0 ms
 Pulse Rate Timing is set to 0 pulses/second
 InterDigit Pulse Duration Timing is set to 0 ms
 Clear Wait Duration Timing is set to 0 ms
 Wink Wait Duration Timing is set to 0 ms
 Wink Duration Timing is set to 0 ms
 Delay Start Timing is set to 0 ms
 Delay Duration Timing is set to 0 ms
```

The following is sample output from the **show voice port** command for a Foreign Exchange Station (FXS) analog voice port on a Cisco 3600:

```
Foreign Exchange Station 1/0/0 Slot is 1, Sub-unit is 0, Port is 0
 Type of VoicePort is FXS
 Operation State is DORMANT
 Administrative State is UP
 The Interface Down Failure Cause is 0
 Alias is NULL
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to 0 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 16ms
 Connection Mode is Normal
 Connection Number is
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
Analog Info Follows:
 Region Tone is set for northamerica
 Currently processing none
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Voice card specific Info Follows:
 Signal Type is loopStart
 Ring Frequency is 25 Hz
 Hook Status is On Hook
 Ring Active Status is inactive
 Ring Ground Status is inactive
 Tip Ground Status is inactive
 Digit Duration Timing is set to 100 ms
 InterDigit Duration Timing is set to 100 ms
 Hook Flash Duration Timing is set to 600 ms
```

The following is sample output from the **show voice port** command for an FXS analog voice port on a Cisco MC3810 multiservice concentrator:

```
Voice port 1/2 Slot is 1, Port is 2
 Type of VoicePort is FXS
 Operation State is UP
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
```

```
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Coder Type is g729ar8
 Companding Type is u-law
 Voice Activity Detection is disabled
 Ringing Time Out is 180 s
 Wait Release Time Out is 30 s
 Nominal Playout Delay is 80 milliseconds
 Maximum Playout Delay is 160 milliseconds

 Analog Info Follows:
 Region Tone is set for northamerica
 Currently processing Voice
 Maintenance Mode Set to None (not in mtc mode)
 Number of signaling protocol errors are 0
 Impedance is set to 600r Ohm
 Analog interface A-D gain offset = -3 dB
 Analog interface D-A gain offset = -3 dB
 Voice card specific Info Follows:
 Signal Type is loopStart
 Ring Frequency is 20 Hz
 Hook Status is On Hook
 Ring Active Status is inactive
 Ring Ground Status is inactive
 Tip Ground Status is active
 Digit Duration Timing is set to 100 ms
 InterDigit Duration Timing is set to 100 ms
 Ring Cadence are [20 40] * 100 msec
 InterDigit Pulse Duration Timing is set to 500 ms
```

The following is sample output from the **show voice port** command for an E&M digital voice port on a Cisco 3600:

```
receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is E&M
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

The following is sample output from the **show voice port summary** command for all voice ports on a Cisco MC3810 multiservice concentrator with an analog voice module (AVM):

```
IN   OUT    ECHO
PORT SIG-TYPE     ADMIN OPER IN-STATUS OUT-STATUS CODEC  VAD GAIN ATTN CANCEL
1/1  fxs-ls       up    up   on-hook   idle       729a    n    0    0    y
1/2  fxs-ls       up    up   on-hook   idle       729a    n    0    0    y
1/3  e&m-wnk      up    up   idle      idle       729a    n    0    0    y
1/4  e&m-wnk      up    up   idle      idle       729a    n    0    0    y
1/5  fxo-ls       up    up   idle      on-hook    729a    n    0    0    y
1/6  fxo-ls       up    up   idle      on-hook    729a    n    0    0    y
```

Table 64 explains the fields in the sample output

Table 64 show voice port Field Descriptions

Field	Description
Administrative State	Administrative state of the voice port.
Alias	User-supplied alias for the voice port.
Analog interface A-D gain offset	Offset of the gain for analog-to-digital conversion.
Analog interface D-A gain offset	Offset of the gain for digital-to-analog conversion.
Clear Wait Duration Timing	Time of inactive seizure signal to declare call cleared.
Coder Type	Voice compression mode used.
Companding Type	Companding standard used to convert between analog and digital signals in PCM systems.
Connection Mode	Connection mode of the interface.
Connection Number	Full E.164 telephone number used to establish a connection with the trunk or PLAR mode.
Currently Processing	Type of call currently being processed: none, voice, or fax.
Delay Duration Timing	Maximum delay signal duration for delay dial signaling.
Delay Start Timing	Timing of generation of delayed start signal from detection of incoming seizure.
Description	Description of the voice port.
Dial Type	Out-dialing type of the voice port.
Digit Duration Timing	DTMF digit duration in milliseconds.
E&M Type	Type of E&M interface.
Echo Cancel Coverage	Echo cancel coverage for this port.
Echo Cancellation	Whether or not echo cancellation is enabled for this port.
Hook Flash Duration Timing	Maximum length of hook flash signal.
Hook Status	Hook status of the FXO/FXS interface.
Impedance	Configured terminating impedance for the E&M interface.
In Gain	Amount of gain inserted at the receiver side of the interface.
In Seizure	Incoming seizure state of the E&M interface.
Initial Time Out	Amount of time the system waits for an initial input digit from the caller.
InterDigit Duration Timing	DTMF interdigit duration, in milliseconds.

Table 64 show voice port Field Descriptions (continued)

Field	Description
InterDigit Pulse Duration Timing	Pulse dialing interdigit timing, in milliseconds.
Interdigit Time Out	Amount of time the system waits for a subsequent input digit from the caller.
Maintenance Mode	Maintenance mode of the voice port.
Maximum Playout Delay	The amount of time before the Cisco MC3810 multiservice concentrator DSP starts to discard voice packets from the digital signal processor (DSP) buffer.
Music On Hold Threshold	Configured Music-On-Hold Threshold value for this interface.
Noise Regeneration	Whether or not background noise should be played to fill silent gaps if VAD is activated.
Nominal Playout Delay	The amount of time the Cisco MC3810 multiservice concentrator DSP waits before starting to play out the voice packets from the DSP buffer.
Non-Linear Processing	Whether or not nonlinear processing is enabled for this port.
Number of signaling protocol errors	Number of signaling protocol errors.
Operations State	Operation state of the port.
Operation Type	Operation of the E&M signal: two-wire or four-wire.
Out Attenuation	Amount of attenuation inserted at the transmit side of the interface.
Out Seizure	Outgoing seizure state of the E&M interface.
Port	Port number for this interface associated with the voice interface card.
Pulse Rate Timing	Pulse dialing rate, in pulses per second (pps).
Region Tone	Configured regional tone for this interface.
Ring Active Status	Ring active indication.
Ring Cadence	Configured ring cadence for this interface.
Ring Frequency	Configured ring frequency for this interface.
Ring Ground Status	Ring ground indication.
Ringing Time Out	Ringing timeout duration.
Signal Type	Type of signaling for a voice port: loop-start, ground-start, wink-start, immediate, and delay-dial.
Slot	Slot used in the voice interface card for this port.
Sub-unit	Subunit used in the voice interface card for this port.
Tip Ground Status	Tip ground indication.
Type of VoicePort	Type of voice port: FXO, FXS, or E&M.
The Interface Down Failure Cause	Text string describing why the interface is down,
Voice Activity Detection	Whether Voice Activity Detection is enabled or disabled.

Table 64 show voice port Field Descriptions (continued)

Field	Description
Wait Release Time Out	The length of time a voice port stays in the call-failure state while the Cisco MC3810 multiservice concentrator sends a busy tone, a reorder tone, or an out-of-service tone to the port.
Wink Duration Timing	Maximum wink duration for wink start signaling.
Wink Wait Duration Timing	Maximum wink wait duration for wink start signaling.

The following example displays voice port configuration information for the digital voice port 0 located in slot 1, DS0 group 1:

```
receEive and transMit Slot is 1, Sub-unit is 0, Port is 1
 Type of VoicePort is E&M
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is not set
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 DBMS
 In Gain is Set to 0 dBm
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 8 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

The following is sample output from the Cisco AS5800 for the **show voice port** command:

```
ISDN 1/0/0:D
 Type of VoicePort is ISDN
 Operation State is DORMANT
 Administrative State is UP
 No Interface Down Failure
 Description is ""
 Noise Regeneration is enabled
 Non Linear Processing is enabled
 Music On Hold Threshold is Set to -38 dBm
 In Gain is Set to 0 dB
 Out Attenuation is Set to 0 dB
 Echo Cancellation is enabled
 Echo Cancel Coverage is set to 16 ms
 Connection Mode is normal
 Connection Number is not set
 Initial Time Out is set to 10 s
 Interdigit Time Out is set to 10 s
 Region Tone is set for US
```

Table 65 describes the significant fields shown in the display.

Table 65 show voice port Field Descriptions for the Cisco AS5800

Field	Description
Type of VoicePort	Indicates the voice port type.
Operational State	Operational state of the voice port.
Administrative State	Administrative state of the voice port.
Clear Wait Duration Timing	Time of inactive seizure signal to declare call cleared.
Currently Processing	Type of call currently being processed: none, voice, or fax.
Operations State	Operation state of the port.
Operation Type	Operation of the E&M signal: two-wire or four-wire.
Noise Regeneration	Whether or not background noise should be played to fill silent gaps if VAD is activated.
Non-Linear Processing	Whether or not nonlinear processing is enabled for this port.
Music-On-Hold Threshold	Configured music-on-hold threshold value for this interface.
In Gain	Amount of gain inserted at the receiver side of the interface.
Out Attenuation	Amount of attenuation inserted at the transmit side of the interface.
Pulse Rate Timing	Pulse dialing rate, in pulses per second (pps).
Echo Cancellation	Whether or not echo cancellation is enabled for this port.
Echo Cancel Coverage	Echo cancel coverage for this port.
Connection Mode	Connection mode of the interface.
Connection Number	Full E.164 telephone number used to establish a connection with the trunk or PLAR mode.
Initial Time Out	Amount of time the system waits for an initial input digit from the caller.
Interdigit Time Out	Amount of time the system waits for a subsequent input digit from the caller.
Regional Tone	Configured regional tone for this interface.

show voice trunk-conditioning signaling

To display the status of trunk-conditioning signaling and timing parameters for a voice port, use the **show voice trunk-conditioning signaling** command in user EXEC or privileged EXEC mode.

show voice trunk-conditioning signaling [**summary** | *voice-port*]

Syntax Description

summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
voice-port	(Optional) Displays a detailed report for a specified voice port.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.0(3)XG	This command was introduced on the Cisco MC3810 multiservice concentrator as **show voice permanent-call**.
12.0(4)T	This command was integrated into the 12.0(4)T release.
12.0(7)XK	This command was renamed **show voice trunk-conditioning signaling**.
12.1(2)T	This command was integrated into the 12.1(2)T release.
12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines

The **show voice trunk-conditioning signaling** command displays the trunk signaling status for analog and digital voice ports on Cisco MC3810 multiservice concentrators and Cisco 2600 and 3600 series routers.

Examples

The following is a sample display from the **show voice trunk-conditioning signaling summary** command for voice ports on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning signaling summary

1/1 is shutdown
1/4 is shutdown
1/5 :
TX INFO :slow-mode seq#= 25, sig pkt cnt= 40, last-ABCD=0000
hardware-state ACTIVE signal type is NorthamericanCAS signal path  is OPEN
RX INFO :slow-mode, sig pkt cnt= 36, prev-seq#= 25, last-ABCD=0000
```

The following is a sample display from the **show voice trunk-conditioning signaling** command for voice port 1/5 on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning signaling 1/5

1/5 :
```

```
TX INFO :slow-mode seq#= 25, sig pkt cnt= 42, last-ABCD=0000
hardware-state ACTIVE signal type is NorthamericanCAS
signal path  is OPEN
 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
 0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
RX INFO :slow-mode, sig pkt cnt= 37
missing = 0, out of seq = 0, very late = 0
playout depth = 0 (ms), refill count = 1
prev-seq#= 25, last-ABCD=0000
trunk_down_timer = 4212 (ms), idle timer = 0 (sec),
tx_oos_timer = 0 (sec), rx_ais_duration = 0 (ms)
forced playout signal pattern = NONE
signaling playout history
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
0000 0000 0000 0000 0000 0000 0000 0000 0000 0000
```

The following is a sample display from the **show voice trunk-conditioning signaling summary** command for voice ports on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning signaling summary

2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8  is shutdown
3/0:1 1  is shutdown
3/0:2 2  is shutdown
3/0:3 3  is shutdown
3/0:5 5  is shutdown
3/0:6(6) :
 status :
3/0:7 7  is shutdown
3/1:0 8  is shutdown
3/1:1 1  is shutdown
3/1:3 3  is shutdown
3/1:5 5  is shutdown
3/1:7 7  is shutdown
```

The following is a sample display from the **show voice trunk-conditioning signaling** command for voice port 3/0:6 on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning signaling 3/0:6

hardware-state ACTIVE signal type is NorthamericanCAS
status :
forced playout pattern = STOPPED
trunk_down_timer = 0, rx_ais_duration = 0, idle_timer = 0
```

Table 66 describes the significant fields shown in the display.

Table 66 show voice trunk-conditioning signaling Field Descriptions

Field	Description
current timer	Time since last signaling packets were received.
forced playout pattern	Which forced playout pattern is sent to PBX: • 0 = no forced playout pattern is sent • 1 = receive IDLE playout pattern is sent • 2 = receive OOS playout pattern is sent
hardware-state	Hardware state based on received IDLE pattern: IDLE = both sides are idle ACTIVE = at least one side is active
signal type	Signaling type used by lower level driver: northamerica, melcas, transparent, or external.
idle timer	Time the hardware on both sides has been in idle state.
last-ABCD	Last received or transmitted signal bit pattern.
max inter-arrival time	Maximum interval between received signaling packets.
missing	Number of missed signal packets.
mode	Signaling packet generation frequency: • fast mode = every 4 milliseconds • slow mode = same frequency as keepalive timer
out of seq	Number of out-of-sequence signal packets.
playout depth	Number of packets in playout buffer.
prev-seq#	Sequence number of previous signaling packet.
refill count	Number of packets created to maintain nominal length of playout packet buffer.
rx_ais_duration	Time since receipt of AIS indicator.
seq#	Sequence number of signaling packet.
sig pkt cnt	Number of transmitted or received signaling packets.
signal path	Status of signaling path.
signaling playout history	Signaling bits received in last 60 milliseconds.
trunk_down_timer	Time since last signaling packets were received.
tx_oos_timer	Time since PBX started sending OOS signaling pattern defined by **signal pattern oos transmit**.
very late	Number of very late signaling packets.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Shows the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning supervisory	Displays the status of trunk supervision and configuration parameters for voice ports.

show voice trunk-conditioning supervisory

To display the status of trunk supervision and configuration parameters for a voice port, use the **show voice trunk-conditioning supervisory** command in user EXEC or privileged EXEC mode.

show voice trunk-conditioning supervisory [**summary** | *voice-port*]

Syntax Description

summary	(Optional) Displays a summary of the status for all voice ports on the router or concentrator.
voice-port	(Optional) Displays a detailed report for a specified voice port.

Command Modes

User EXEC

Privileged EXEC

Command History

Release	Modification
12.0(7)XK	This command was introduced on the Cisco 2600 and 3600 series routers, and the MC3810 multiservice concentrator.
12.1(2)T	This command was integrated into the 12.1(2)T release.
12.1(3)T	This command was first supported on the Cisco 2600 and 3600 series routers.

Usage Guidelines

The **show voice trunk-conditioning supervisory** command displays the trunk supervision and configuration status for analog and digital voice ports.

Examples

The following is a sample display from the **show voice trunk-conditioning supervisory summary** command for voice ports on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning supervisory summary

1/1 is shutdown
1/4 is shutdown
1/5 : state : TRUNK_SC_CONNECT, voice : on , signal : on ,slave
```

The following is a sample display from the **show voice trunk-conditioning supervisory** command for voice port 1/5 on a Cisco MC3810 multiservice concentrator:

```
Router# show voice trunk-conditioning supervisory 1/5

1/5 : state : TRUNK_SC_CONNECT, voice : on, signal : on, slave
status: trunk connected
sequence oos : idle and oos
pattern :rx_idle = 0x0 rx_oos = 0xF tx_oos =  0xF
timing : idle = 0, restart = 0, standby = 0, timeout = 40
supp_all = 50, supp_voice = 0, keep_alive = 5
timer: oos_ais_timer = 0, timer = 0
```

The following is a sample display from the **show voice trunk-conditioning supervisory summary** command for voice ports on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning supervisory summary

2/0/0 is shutdown
2/0/1 is shutdown
3/0:0 8  is shutdown
3/0:1 1  is shutdown
3/0:2 2  is shutdown
3/0:3 3  is shutdown
3/0:5 5  is shutdown
3/0:6(6) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/0:7(7) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:0(8) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:1(1) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:3(3) : state : TRUNK_SC_CONNECT, voice : on , signal : on ,master
3/1:5(5) is shutdown
3/1:7(7) is shutdown
```

The following is a sample display from the **show voice trunk-conditioning supervisory** command for voice port 3/0:6 on a Cisco 3600 series router:

```
Router# show voice trunk-conditioning supervisory 3/0:6

3/0:6(6) : state : TRUNK_SC_CONNECT, voice : on, signal : on, master
status: trunk connected
sequence oos : idle and oos
pattern :rx_idle = 0x0 rx_oos = 0xF
timing : idle = 0, restart = 0, standby = 0, timeout = 40
supp_all = 0, supp_voice = 0, keep_alive = 5
timer: oos_ais_timer = 0, timer = 0
```

Table 67 describes the significant fields shown in the display.

Table 67 show voice trunk-conditioning supervisory Field Descriptions

Field	Description
keep_alive	Signaling packets periodically sent to the far end, even if there is no signal change. These signaling packets function as keep alive messages.
master	The voice port configured as "connect trunk xxxx."
slave	The voice port configured as "connect trunk xxxx answer-mode."
oos_ais_timer	Time since the signaling packet with AIS indicator was received.
pattern	4-bit signaling pattern.
restart	The restart timeout after far end is OOS.
rx-idle	The signaling bit pattern indicating that the far end is idle.
rx-oos	The signaling bit pattern sent to the PBX indicating that the network is OOS.
standby	The time before the slave side goes back to standby after the far end goes OOS.
supp_all	The timeout before suppressing transmission of voice and signaling packets to the far end after detection of PBX OOS.
supp_voice	The timeout before suppressing transmission of voice packet to the far end after detection of PBX oos.
timeout	The timeout for nonreceipt of keepalive packets before the far end is considered to be OOS.
TRUNK_SC_CONNECT	Trunk conditioning supervisory component status.

Related Commands

Command	Description
show dial-peer voice	Displays the configuration for all VoIP and POTS dial peers configured on the router.
show voice dsp	Displays the current status of all DSP voice channels.
show voice port	Displays configuration information about a specific voice port.
show voice trunk-conditioning signaling	Displays the status of trunk-conditioning signaling and timing parameters for a voice port

show vrm active_calls

To display active-only voice calls either for a specific voice feature card (VFC) or for all VFCs, use the **show vrm active_calls** command in privileged EXEC mode.

show vrm active_calls {*dial-shelf-slot-number* | **all**}

Syntax Description

dial-shelf-slot-number	Slot number of the dial shelf. Valid number is 0 to 13.
all	Lists all active calls for VFC slots.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800 universal access server.

Usage Guidelines

Use the **show vrm active_calls** to display active-only voice calls either for a specific VFC or for all VFCs. Each active call occupies a block of information describing the call. This information provides basically the same information as the **show vrm vdevice** command.

Examples

The following is sample output from the **show vrm active_calls** command specifying dial shelf slot number:

```
Router# show vrm active_calls 6

slot =  6 virtual voice dev (tag) =  61 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 241
Resource (vdev_common) status = 401 means :active others
tot ingress data =  24
tot ingress control  = 1308
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 22051
tot egress control  = 1304
tot egress data drops  = 0
tot egress control drops  = 0

slot =  6 virtual voice dev (tag) =  40 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 157
Resource (vdev_common) status = 401 means :active others
```

Table 68 describes the significant fields shown in the display.

Table 68 show vrm active_calls Field Descriptions

Field	Description
slot	Slot where voice card is installed.
virtual voice dev (tag)	Identification number of the virtual voice device.
channel id	Identification number of the channel associated with this virtual voice device.
capability list map	Bitmaps for the codec supported on that DSP channel. Available values are: CC_CAP_CODEC_G711U: 0x1 CC_CAP_CODEC_G711A: 0x2 CC_CAP_CODEC_G729IETF: 0x4 CC_CAP_CODEC_G729a: 0x8 CC_CAP_CODEC_G726r16: 0x10 CC_CAP_CODEC_G726r24: 0x20 CC_CAP_CODEC_G726r32: 0x40 CC_CAP_CODEC_G728: 0x80 CC_CAP_CODEC_G723r63: 0x100 CC_CAP_CODEC_G723r53: 0x200 CC_CAP_CODEC_GSM: 0x400 CC_CAP_CODEC_G729b: 0x800 CC_CAP_CODEC_G729ab: 0x1000 CC_CAP_CODEC_G723ar63: 0x2000 CC_CAP_CODEC_G723ar53: 0x4000 CC_CAP_CODEC_G729: 0x8000
last/current codec loaded/used	Indicates the last codec loaded or used.
TDM time slot	Time division multiplexing time slot.
Resource (vdev_common) status	Current status of the VFC.
tot ingress data	Total amount of data (number of packets) sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the Voice over IP (VoIP) side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.

Table 68 show vrm active_calls Field Descriptions (continued)

Field	Description
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

Related Commands

Command	Description
show vrm vdevices	Displays detailed information for a specific DSP or a brief summary display for all VFCs.

show vrm vdevices

To display detailed information for a specific digital signal processor (DSP) or a brief summary display for all voice feature cards (VFCs), use the **show vrm vdevices** command in privileged EXEC mode.

show vrm vdevices {{*vfc-slot-number* | *voice-device-number*} | **summary**}

Syntax Description

vfc-slot-number	Slot number of the VFC. Valid number is from 0 to 11.
voice-device-number	DSP number. Valid number is from 1 to 96.
summary	List synopsis of voice feature card DSP mappings, capabilities, and resource states.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(7)T	This command was introduced on the Cisco AS5800 universal access server.

Usage Guidelines

Use the **show vrm vdevices** command to display detailed information for a specific DSP or a brief summary display for all VFCs. The display provides information on the number of channels, channels per DSP, bitmap of DSPMs, version numbers, and so on. This information is useful in monitoring the current state of your VFCs.

The display for a specific DSP provides information on the codec that each channel is using, if active, or last used and if the channel is not currently sending cells. It also displays the state of the resource. In most cases, if there is an active call on that channel, the resource should be marked active. If the resource is marked as reset or bad, this may be an indication of a response loss for the VFC on a reset request. If this condition persists, you might experience a problem with the communication link between the router shelf and the VFC.

Examples

The following is sample output from the **show vrm vdevices** command specifying dial shelf slot number and DSP number. In this particular example, the call is active so the statistics displayed are for this active call. If no calls are currently active on the device, the statistics would be for the previous (or last active) call.

```
Router# show vrm vdevices 6 1

slot =  6 virtual voice dev (tag) =  1 channel id = 1
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 0
Resource (vdev_common) status = 401 means :active others
tot ingress data =  101
```

```
tot ingress control  = 1194
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 39722
tot egress control  = 1209
tot egress data drops  = 0
tot egress control drops  = 0

slot =  6 virtual voice dev (tag) =  1 channel id = 2
capabilities list map = 9FFF
last/current codec loaded/used = None
TDM timeslot = 1
Resource (vdev_common) status = 401 means :active others
tot ingress data =  21
tot ingress control  = 1167
tot ingress data drops  = 0
tot ingress control drops  = 0
tot egress data  = 19476
tot egress control  = 1163
tot egress data drops  = 0
tot egress control drops  = 0
```

Table 69 describes the significant fields shown in the display.

Table 69 show vrm vdevices Field Descriptions

Field	Description
slot	Slot where voice card is installed.
virtual voice dev (tag)	Identification number of the virtual voice device.
channel id	Identification number of the channel associated with this virtual voice device.

Table 69 show vrm vdevices Field Descriptions (continued)

Field	Description
capability list map	Bitmaps for the codec supported on that DSP channel. Available values are: • CC_CAP_CODEC_G711U: 0x1 • CC_CAP_CODEC_G711A: 0x2 • CC_CAP_CODEC_G729IETF: 0x4 • CC_CAP_CODEC_G729a: 0x8 • CC_CAP_CODEC_G726r16: 0x10 • CC_CAP_CODEC_G726r24: 0x20 • CC_CAP_CODEC_G726r32: 0x40 • CC_CAP_CODEC_G728: 0x80 • CC_CAP_CODEC_G723r63: 0x100 • CC_CAP_CODEC_G723r53: 0x200 • CC_CAP_CODEC_GSM: 0x400 • CC_CAP_CODEC_G729b: 0x800 • CC_CAP_CODEC_G729ab: 0x1000 • CC_CAP_CODEC_G723ar63: 0x2000 • CC_CAP_CODEC_G723ar53: 0x4000 • CC_CAP_CODEC_G729: 0x8000
last/current codec loaded/used	The last codec loaded or used.
TDM time slot	Time division multiplexing time slot.

Table 69 show vrm vdevices Field Descriptions (continued)

Field	Description
Resource (vdev_common) status	Current status of the VFC. Possible field values are: • FREE = 0x0000 • ACTIVE_CALL = 0x0001 • BUSYOUT_REQ = 0x0002 • BAD = 0x0004 • BACK2BACK_TEST = 0x0008 • RESET = 0x0010 • DOWNLOAD_FILE = 0x0020 • DOWNLOAD_FAIL = 0x0040 • SHUTDOWN = 0x0080 • BUSY = 0x0100 • OIR = 0x0200 • HASLOCK = 0x0400 /* vdev_pool has locked port */ • DOWNLOAD_REQ = 0x0800 • RECOVERY_REQ = 0x1000 • NEGOTIATED = 0x2000 • OOS = 0x4000
tot ingress data	Total amount of data (number of packets) sent from the PSTN side of the connection to the Voice over IP (VoIP) side of the connection.
tot ingress control	Total number of control packets sent from the PSTN side of the connection to the VoIP side of the connection.
tot ingress data drops	Total number of data packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot ingress control drops	Total number of control packets dropped from the PSTN side of the connection to the VoIP side of the connection.
tot egress data	Total amount of data (number of packets) sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress control	Total number of control packets sent from the VoIP side of the connection to the PSTN side of the connection.
tot egress data drops	Total number of data packets dropped from the VoIP side of the connection to the PSTN side of the connection.
tot egress control drops	Total number of control packets dropped from the VoIP side of the connection to the PSTN side of the connection.

The following is sample output from the **show vrm devices** command specifying a summary list. In the “Voice Device Mapping” area, the “C_Ac” column indicates number of active calls for a specific DSP. If there are any nonzero numbers under the “C_Rst” and/or “C_Bad” column, this indicates that a reset request was sent but it was lost; this could mean a faulty DSP.

```
Router# show vrm vdevices summary
```

```
**********************************************************
******summary of voice devices for all voice cards*********
**********************************************************

slot = 6 major ver = 0 minor ver = 1 core type used = 2
number of modules = 16 number of voice devices (DSPs) = 96
chans per vdevice = 2 tot chans = 192 tot active calls = 178
module presense bit map = FFFF tdm mode = 1 num_of_tdm_timeslots = 384
auto recovery is on

number of default voice file (core type images) = 2
file 0 maj ver = 0 min ver = 0 core_type = 1
trough size = 2880 slop value = 0 built-in codec bitmap = 0
loadable codec bitmap = 0 fax codec bitmap = 0

file 1 maj ver = 3 min ver = 1 core_type = 2
trough size = 2880 slop value = 1440 built-in codec bitmap = 40B
loadable codec bitmap = BFC fax codec bitmap = 7E


-------------------Voice Device Mapping------------------------
Logical Device (Tag)  Module#  DSP#  C_Ac  C_Busy  C_Rst  C_Bad
--------------------------------------------------------------
1                     1         1     2     0       0      0
2                     1         2     2     0       0      0
3                     1         3     2     0       0      0
4                     1         4     2     0       0      0
5                     1         5     2     0       0      0
6                     1         6     2     0       0      0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
7                     2         1     2     0       0      0
8                     2         2     2     0       0      0
9                     2         3     2     0       0      0
10                    2         4     1     0       0      0
11                    2         5     2     0       0      0
12                    2         6     1     0       0      0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
<information deleted>
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
91                    16        1     2     0       0      0
92                    16        2     2     0       0      0
93                    16        3     1     0       0      0
94                    16        4     2     0       0      0
95                    16        5     2     0       0      0
96                    16        6     2     0       0      0
++++++++++++++++++++++++++++++++++++++++++++++++++++++++++

Total active call channels = 178
Total busied out channels = 0
Total channels in reset = 0
Total bad channels = 0
Note :Channels could be in multiple states
```

Table 70 describes the significant fields shown in the display.

Table 70 show vrm vdevices summary Field Descriptions

Field	Description
slot	Slot number where VFC is installed.
major ver	Major version of firmware running on VFC.
minor ver	Minor version of firmware running on VFC.

Table 70 show vrm vdevices summary Field Descriptions (continued)

Field	Description
core type used	Type of DSPware in use. Possible field values are: • 1 = UBL (boot loader) • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core • 255 = invalid
number of modules	Number of modules on the VFC. Maximum is 16.
number of voice devices (DSP)s	Number of possible DSPs. Maximum number is 96.
chans per vdevice	Number of channels (meaning calls) each DSP can handle.
tot chans	Total number of channels.
tot active calls	Total number of active calls on this VFC.
module presense bit map	Indicates a 16-bit bitmap, each bit representing a module.
tdm mode	Time division multiplex bus mode. Possible field values are: • 0 = VFC is in classic mode. • 1 = VFC is in plus mode. This field should always be 1.
num_of_tdm_time slots	Total number of calls that can be handled by the VFC.
auto recovery	Indicates whether auto recovery is enabled. When autorecovery is enabled, the VRM will try to recover a DSP by resetting it if, for some reason, the DSP stops responding.
number of default voice file (core type images)	Number of DSPware files in use.
maj ver	Major version of the DSPware in use.
min ver	Minor version of the DSPware in use.
core type	Type of DSPware in use: Possible field values are: • 1 = boot loader • 2 = high complexity core • 3 = medium complexity core • 4 = low complexity core
trough size	This value indirectly represents the complexity of the DSPware in use.
slop value	This value indirectly represents the complexity of the DSPware in use.

Table 70 show vrm vdevices summary Field Descriptions (continued)

Field	Description
built-in codec bitmap	Represents the bitmap of the codec built into the DSP firmware. Possible field values are: • CC_CAP_CODEC_G711U 0x0001 • CC_CAP_CODEC_G711A 0x0002 • CC_CAP_CODEC_G729IETF 0x0004 • CC_CAP_CODEC_G729a 0x0008 • CC_CAP_CODEC_G726r16 0x0010 • CC_CAP_CODEC_G726r24 0x0020 • CC_CAP_CODEC_G726r32 0x0040 • CC_CAP_CODEC_G728 0x0080 • CC_CAP_CODEC_G723r63 0x0100 • CC_CAP_CODEC_G723r53 0x0200 • CC_CAP_CODEC_GSM 0x0400 • CC_CAP_CODEC_G729b 0x0800 • CC_CAP_CODEC_G729ab 0x1000 • CC_CAP_CODEC_G723ar63 0x2000 • CC_CAP_CODEC_G723ar53 0x4000 • CC_CAP_CODEC_G729 0x8000
loadable codec bitmap	Represents the loadable codec bitmap for the loadable codecs. Possible field values are: • CC_CAP_CODEC_G711U = 0x0001 • CC_CAP_CODEC_G711A = 0x0002 • CC_CAP_CODEC_G729IETF = 0x0004 • CC_CAP_CODEC_G729a = 0x0008 • CC_CAP_CODEC_G726r16 = 0x0010 • CC_CAP_CODEC_G726r24 = 0x0020 • CC_CAP_CODEC_G726r32 = 0x0040 • CC_CAP_CODEC_G728 = 0x0080 • CC_CAP_CODEC_G723r63 = 0x0100 • CC_CAP_CODEC_G723r53 = 0x0200 • CC_CAP_CODEC_GSM = 0x0400 • CC_CAP_CODEC_G729b = 0x0800 • CC_CAP_CODEC_G729ab = 0x1000 • CC_CAP_CODEC_G723ar63 = 0x2000 • CC_CAP_CODEC_G723ar53 = 0x4000 • CC_CAP_CODEC_G729 = 0x8000

Table 70 show vrm vdevices summary Field Descriptions (continued)

Field	Description
fax codec bitmap	Represents the fax codec bitmap. Possible field values are: • FAX_NONE = 0x1 • FAX_VOICE = 0x2 • FAX_144 = 0x4 • FAX_96 = 0x8 • FAX_72 = 0x10 • FAX_48 = 0x20 • FAX_24 = 0x40
Logical Device (Tag)	Tag number or DSP number on that VFC.
Module #	Number identifying the module associated with a specific logical device.
DSP#	Number identifying the DSP on the VFC.
C_Ac	Number of active calls on identified DSP.
C_Busy	Number of busied-out channels associated with identified DSP.
C_Rst	Number of channels in the reset state associated with identified DSP.
C_Bad	Number of defective ("bad") channels associated with identified DSP.
Total active call channels	Total number of active calls.
Total busied out channels	Total number of busied-out channels.
Total channels in reset	Total number of channels in reset state.
Total bad channels	Total number of defective channels.

Related Commands

Command	Description
show vrm active_calls	Displays active-only voice calls for either a specific VFC or all VFCs.

shut

To shut down a set of digital signal processors (DSPs) on the Cisco 7200 series router, use the **shut** command in DSP configuration mode. To put DSPs back in service, use the **no** form of this command.

shut *number*

no shut *number*

Syntax Description

number	Number of DSPs to be shut down.

Defaults

no shut

Command Modes

DSP configuration

Command History

Release	Modification
12.0(5)XE	This command was introduced on the Cisco 7200 series router.
12.1(1)T	This command was modified to add information about DSP groups.

Usage Guidelines

This command applies to Voice over IP on the Cisco 7200 series routers.

Examples

The following example shuts down two sets of DSPs:

```
shut 2
```

shutdown (dial-peer)

To change the administrative state of the selected dial peer from up to down, use the **shutdown** command in dial-peer configuration mode. To change the administrative state of this dial peer from down to up, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

no shutdown

Command Modes

Dial-peer configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.
12.1(1)	This command was modified for store-and-forward fax.

Usage Guidelines

When a dial peer is shut down, you cannot initiate calls to that peer.

This command applies to both on-ramp and off-ramp store-and-forward fax functions.

Examples

The following example changes the administrative state of voice telephony (plain old telephone service [POTS]) dial peer 10 to down:

```
dial-peer voice 10 pots
shutdown
```

The following example changes the administrative state of voice telephony (POTS) dial peer 10 to up:

```
dial-peer voice 10 pots
no shutdown
```

Related Commands

Command	Description
dial-peer voice	Enters dial-peer configuration mode, defines the type of dial peer, and defines the dial-peer tag number.

shutdown (DS1)

To shut down a DS1 link (send a Blue Alarm), use the **shutdown** command in controller configuration mode. To activate the DS1 (cancel the sending of the Blue Alarm), use the **no** form of the command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

no shutdown

Command Modes

Controller configuration

Command History

Release	Modification
11.3(1)MA	This command was introduced.

Usage Guidelines

This command applies to Voice over Frame Relay and Voice over ATM on the Cisco MC3810 multiservice concentrator.

Examples

The following example shuts down a DS1 link on controller T1 0:

```
controller T1 0
 shutdown
```

shutdown (gatekeeper)

To disable the gatekeeper, use the **shutdown** command in gatekeeper configuration mode. To enable the gatekeeper, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled (shut down)

Command Modes

gatekeeper configuration

Command History

Release	Modification
11.3(2)NA	This command was introduced on the Cisco 2500 series and Cisco 3600 series routers.
12.0(3)T	The command was integrated into Cisco IOS Release 12.0(3)T and supported on the Cisco MC3810 multiservice concentrator.

Usage Guidelines

The gatekeeper does not have to be enabled before you can use the other gatekeeper configuration commands. In fact, it is recommended that you complete the gatekeeper configuration before bringing up the gatekeeper because some characteristics may be difficult to alter while the gatekeeper is running, as there may be active registrations or calls.

The **no shutdown** command enables the gatekeeper, but it does not make the gatekeeper operational. The two exceptions to this are as follows:

- If no local zones are configured, a **no shutdown** command places the gatekeeper in INACTIVE mode waiting for a local zone definition.
- If local zones are defined to use an HSRP virtual address, and the HSRP interface is in STANDBY mode, the gatekeeper goes into HSRP STANDBY mode. Only when the HSRP interface is ACTIVE will the gatekeeper go into the operational UP mode.

Examples

The following command disables a gatekeeper:

```
shutdown
```

shutdown (RLM)

To shut down all of the links under the RLM group, use the **shutdown** command in RLM configuration mode. RLM will not try to reestablish those links until the command is negated. To disable this function, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

RLM configuration

Command History

Release	Modification
11.3(7)	This command was introduced.

Related Commands

Command	Description
clear rlm group	Clears all RLM group time stamps to zero.
clear interface	Resets the hardware logic on an interface.
interface	Defines the IP addresses of the server, configures an interface type, and enters interface configuration mode.
link (RLM)	Specifies the link preference.
protocol rlm port	Reconfigures the port number for the basic RLM connection for the whole rlm-group.
retry keepalive	Allows consecutive keepalive failures a certain amount of time before the link is declared down.
server (RLM)	Defines the IP addresses of the server.
show rlm group statistics	Displays the network latency of the RLM group.
show rlm group status	Displays the status of the RLM group.
show rlm group timer	Displays the current RLM group timer values.
timer	Overwrites the default setting of timeout values.

shutdown (settlement)

To deactivate the settlement provider, use the **shutdown** command in settlement configuration mode. To activate a settlement provider, use the **no shutdown** command

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

The default status of a settlement provider is deactivated. The settlement provider is down.

Command Modes

Settlement configuration

Command History

Release	Modification
12.0(4)XH1	This command was introduced the Cisco 2500 series and Cisco 3600 series routers and on the Cisco AS5300 universal access server.
12.1(1)T	This command was integrated into Cisco IOS Release 12.1(1)T.

Usage Guidelines

Use the **no shutdown** command at the end of the configuration of a settlement server to bring up the provider. This command activates the provider. Otherwise, transactions will not go through the provider to be audited and charged. Use the **shutdown** command to deactivate the provider.

Examples

The following example enables a settlement server:

```
settlement 0
 no shutdown
```

The following example disables a settlement server:

```
settlement 0
 shutdown
```

Related Commands

Command	Description
connection-timeout	Configures the time that a connection is maintained after completing a communication exchange.
customer-id	Identifies a carrier or ISP with a settlement provider.
device-id	Specifies a gateway associated with a settlement provider.
encryption	Sets the encryption method to be negotiated with the provider.
max-connection	Sets the maximum number of simultaneous connections to be used for communication with a settlement provider.

Command	Description
response-timeout	Configures the maximum time to wait for a response from a server.
retry-delay	Sets the time between attempts to connect with the settlement provider.
session-timeout	Sets the interval for closing the connection when there is no input or output traffic.
settlement	Enters settlement configuration mode and specifies the attributes specific to a settlement provider.
type	Configures an SAA-RTR operation type.

shutdown (voice-port)

To take the voice ports for a specific voice interface card offline, use the **shutdown** command in voice-port configuration mode. To put the ports back in service, use the **no** form of this command.

shutdown

no shutdown

Syntax Description

This command has no arguments or keywords.

Defaults

shutdown

Command Modes

Voice-port configuration

Command History

Release	Modification
11.3(1)T	This command was introduced on the Cisco 3600 series router.

Usage Guidelines

When you enter the **shutdown** command, all ports on the voice interface card are disabled. When you enter the **no shutdown** command, all ports on the voice interface card are enabled. A telephone connected to an interface will hear dead silence when a port is shut down.

Examples

The following example takes voice port 1/1/0 on the Cisco 3600 series offline:

```
voice-port 1/1/0
shutdown
```

Note The preceding configuration example shuts down both voice ports 1/1/0 and 1/1/1.